ANEXO 2:

REQUISITOS DE SEGURIDAD PARA LA ACREDITACIÓN

REQUISITOS DE SEGURIDAD PARA LA ACREDITACIÓN

1. Resumen de Requisitos Adicionales de Acreditación

POLÍTICA DE SEGURIDAD	
1.NOMBRE	Aseguramiento y Documentación de la Política de Seguridad.
CÓDIGO DE REQUISITO	PS01.
DEPENDENCIA	Ninguna.
ESTANDARES	NTP-ISO/IEC 17799, ISO 27001, BS 7799-II.
DOCUMENTACIÓN SOLICITADA[1]	Política de Seguridad.
EVIDENCIAS SOLICITADAS[2]	Política de Seguridad.
2.NOMBRE	Registro, Verificación y Valoración del Análisis de Riesgos y Amenazas.
CÓDIGO DE REQUISITO	PS02.
DEPENDENCIA	PS01.
ESTANDARES	NTP-ISO/IEC 17799, ISO 27001, BS 7799-II.
DOCUMENTACIÓN SOLICITADA	Valoración de riesgos.
EVIDENCIAS SOLICITADAS	Informe Auditor Independiente.
3.NOMBRE	Continuidad del Negocio y Recuperación de Desastres.
CÓDIGO DE REQUISITO	PS03.
DEPENDENCIA	PS02.
ESTANDARES S	NTP-ISO/IEC 17799, ISO 27001, ETSI TS 102 042.
DOCUMENTACIÓN SOLICITADA	Plan de Continuidad del Negocio. Plan de Recuperación de Desastres.
EVIDENCIAS SOLICITADAS	Ninguna.
4.NOMBRE	Documentación, Mantenimiento y Planificación de Seguridad del Sistema de Información y Administración de claves.
CÓDIGO DE REQUISITO	PS04.
DEPENDENCIA	PS02.
ESTANDARES	NTP-ISO/IEC 17799, ISO 27001.
DOCUMENTACIÓN SOLICITADA	Plan de Seguridad del Sistema de Información. Plan de Administración de Claves.
EVIDENCIAS SOLICITADAS	Ninguna.

[1] Se refiere a la documentación que debe ser presentada en el proceso de auditoría externa.
[2] Se refiere a la documentación que debe ser presentada a INDECOPI, durante el proceso de acreditación de la EC.

5.NOMBRE CÓDIGO DE REQUISITO DEPENDENCIA ESTANDARES DOCUMENTACIÓN SOLICITADA EVIDENCIAS SOLICITADAS	Evaluación de la Implementación del Plan de Seguridad de los Sistemas de Información. PS05. PS03. NTP-ISO/IEC 17799, ISO 27001. Ninguna. Informe Auditor Independiente.
6.NOMBRE CÓDIGO DE REQUISITO DEPENDENCIA ESTANDARES DOCUMENTACIÓN SOLICITADA EVIDENCIAS SOLICITADAS	Evaluación del Plan de Administración de Claves. PS06. PS04. NTP-ISO/IEC 17799, ISO 27001, ETSI TS 102 042. Ninguna. Informe Auditor Independiente.
CAPACIDAD TECNOLÓGICA	
1.NOMBRE CÓDIGO DE REQUISITO DEPENDENCIA ESTANDARES DOCUMENTACIÓN SOLICITADA EVIDENCIAS SOLICITADAS	Evaluación y Certificación de la Plataforma Tecnológica del PSC. CT01. PS03, PS04, PS05. ITSEC 102 042, FIPS 140-1 o ISO/IEC 15408. Documento de Cumplimiento de Estándares Tecnológicos. Manuales de los fabricantes de los productos hardware y software presentes en la infraestructura. Informe Auditor Independiente. Documento de Cumplimiento de Estándares Tecnológicos.

SEGURIDAD FÍSICA	
1.NOMBRE CÓDIGO DE REQUISITO DEPENDENCIA ESTANDARES DOCUMENTACIÓN SOLICITADA EVIDENCIAS SOLICITADAS	Seguridad física y ambiental de la infraestructura del PSC. SF01. PS04. ISO/IEC 17799, ISO 27001, BS 7799-II, ETSI TS 102 042. Plan de Seguridad Física y Ambiental. Informe Auditor Independiente.
REQUERIMIENTOS DE PERSONAL	
1.NOMBRE CÓDIGO DE REQUISITO DEPENDENCIA ESTANDARES DOCUMENTACIÓN SOLICITADA EVIDENCIAS SOLICITADAS	Evaluación completa de los perfiles del personal al nivel Altamente Confiable. RP01. PS04. ISO/IEC 17799, ISO 27001, BS 7799-II, ETSI TS 102 042. Documento de evaluación de personal. Informe Auditor Independiente.
2.NOMBRE CÓDIGO DE REQUISITO DEPENDENCIA ESTANDARES DOCUMENTACIÓN SOLICITADA EVIDENCIAS SOLICITADAS	Evaluación del Oficial de Seguridad (IT Security Manager). RP02. PS04. ISO 17799, ISO 27001, BS 7799-II. Documento de Evaluación del Oficial de Seguridad. Informe Auditor Independiente.

2. Detalle de Requisitos de Acreditación

2.1 REQUISITO PS01 – ASEGURAMIENTO Y DOCUMENTACIÓN DE LA POLÍTICA DE SEGURIDAD

2.1.1 ESPECIFICACIONES

Nombre	Aseguramiento y Documentación de la Política de Seguridad
Objetivo	Verificar por medio de este documento los objetivos de seguridad de las PSC. Verificar que todos los organismos de gestión de la PSC comprenden, entienden y apoyan esta política.
Descripción	La Política de Seguridad es una declaración de objetivos de seguridad realizables en la amplitud y alcance establecidos, a través de métodos, acciones, procedimientos y mecanismos implementados por el PSC y documentados en su POLÍTICA DE SEGURIDAD. Si el PSC necesita confiar algún aspecto de seguridad o confianza a organizaciones externas, esto debe indicarse claramente en su POLÍTICA DE SEGURIDAD. La POLÍTICA DE SEGURIDAD debe cumplir, como mínimo, con los siguientes requerimientos: • Debe estar basada en las recomendaciones del estándar NTP-ISO/ 17799 sección 3 o ISO 27001. • Sus objetivos deben ser de alto nivel y no técnicos; lo suficientemente general para permitir el uso de alternativas de implementación tecnológica. • Si la complejidad de los objetivos así lo requieren, la POLÍTICA DE SEGURIDAD puede estar conformada por más de un documento; es decir, puede haber una POLÍTICA GENERAL DE SEGURIDAD soportada por POLÍTICAS ESPECÍFICAS DE SEGURIDAD. • Los elementos de la POLÍTICA DE SEGURIDAD que estén incorporados tanto en la Declaración de Prácticas de Certificación (CPS) como en la Política de Certificación (CP) deben estar incluidos en este documento. • Identificar los objetivos de seguridad relevantes y las amenazas potenciales relacionadas a los servicios suministrados, así como las medidas tomadas para evitar los efectos de estas amenazas.

	• Adicionalmente, se recomienda que la documentación describa las reglas, directivas y procedimientos que indican como son provistos los servicios específicos y las medidas de seguridad asociadas. • En el anexo 4 de la Guía de Acreditación de EC se describen los principales aspectos que una política de seguridad debe considerar. Para los propósitos de la acreditación de un PSC, algunos de los aspectos más relevantes han sido incorporados en criterios separados para así facilitar el proceso de evaluación. Por ello, este documento puede expresar en forma general aquellos aspectos de la seguridad organizacional que se tratan en documentos específicos.
Dependencias	NO TIENE
Estándares de evaluación	NTP-ISO/IEC 17799, BS 7799-II, ISO IEC 27001.
Documentación solicitada	Política de Seguridad.
Evidencias solicitadas	Informe de auditor independiente, en terreno que permita verificar el cumplimiento de los objetivos de la POLÍTICA DE SEGURIDAD.

2.1.2 ASPECTOS/CONTROLES ESPECÍFICOS A EVALUAR

Aspecto/Controles	Evaluación
Conformidad con el estándar NTP-ISO/IEC 17799 sección 5. **ISO 27001 sección 5.**	Verificar que los requerimientos de la sección 5 descritos en el anexo 5 estén incorporados.
Conformidad con el estándar NTP-ISO/IEC 17799 sección 5.1.2 **ISO 27001 sección**	Verificar que se ha incluido un procedimiento de revisión y evaluación periódico de la POLÍTICA DE SEGURIDAD.
Consistencia entre la política de seguridad y la CPS	Verificar la consistencia de la POLÍTICA DE SEGURIDAD con la CPS.

Relación entre la valoración riesgos y la política de seguridad	Verificar que los principales aspectos de la POLÍTICA DE SEGURIDAD sean coherentes con los niveles de riesgo determinados en la Valoración de Riesgos.
Inclusión de las secciones pertinentes[3] en el anexo 4 de la Guía de Acreditación EC	Verificar que los elementos fundamentales de una POLÍTICA DE SEGURIDAD estén incluidos en el documento.
Claridad de los objetivos de seguridad	Verificar que se establezcan objetivos de seguridad concretos relacionados con la protección de los procesos de negocios, activos y servicios del PSC.

[3] Internet Security Policy: A Technical Guide, by the National Institute of Standards and Technologies (NIST) http://csrc.nist.gov/nissc/1997/panels/isptg/bagwill/html/
Information Security Policies Made Easy, by Charles Cresson Wood, 8th Ed., Baseline Software, 2001. http://www.baselinesoft.com

2.2 REQUISITO PS02 – REGISTRO, VERIFICACIÓN Y VALORACIÓN DEL ANÁLISIS DE RIESGOS

2.2.1 ESPECIFICACIONES

Nombre	Registro, Verificación y Valoración del Análisis de Riesgos.
Objetivo	Identificación y verificación de la coherencia del análisis de riesgos y amenazas del plan de negocios del PSC.
Descripción	La valoración de riesgos debe identificar, cuantificar y priorizar riesgos contra el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados deben guiar y determinar la apropiada acción de gestión y las prioridades para manejar la información de los riesgos de seguridad y para seleccionar controles que puedan ser implementados seleccionados para proteger estos riesgos. El proceso de valoración de riesgos y de seleccionar controles puede requerir que sea realizado un número significativo de veces con el fin de cubrir diferentes partes de la organización o sistemas de información individuales. El objetivo principal de un proceso de valoración de riesgo en una organización debe ser proteger la organización y su capacidad de cumplir con su misión, además de proteger sus activos IT. La valoración del riesgo incluye tres procesos: 1. Valoración de los riesgos, el cual incluye la identificación y evaluación de impactos de los riesgos. 2. Acciones correctivas, el cual se refiere a la priorización, implementación y manutención de las medidas de reducción de riesgo apropiadas recomendadas por el proceso de valorización de riesgos. Este proceso conduce a la definición de un Plan de Seguridad. 3. Revisión y monitoreo de la valoración de riesgos, que corresponde al proceso de evaluación continua para adecuar dicho proceso a condiciones cambiantes del entorno o del negocio. El resultado debe ser un compromiso razonable entre los costos económicos y operacionales de las medidas de protección con el fin de obtener mejoras en la capacidad de lograr la misión de la organización. Se recomienda seguir un proceso similar al descrito en los documentos indicados en las referencias para realizar el proceso de valoración de riesgos.

Dependencias	PS01
Estándares de evaluación	NTP-ISO/IEC 17799, BS 7799-II, ISO IEC 27001.
Documentación solicitada	Valoración de Riesgos.
Evidencias solicitadas	Informe Auditor Independiente.

2.2.2 ASPECTOS/CONTROLES ESPECÍFICOS A EVALUAR

Aspectos/Controles	**Evaluación**
Conformidad con el estándar NTP-ISO/IEC 17799 Sección 14.1.2 ISO 27001 sección 14.1.2	Verificar que se logren identificar y evaluar los riesgos, de acuerdo a estándares internacionales.
Reporte de la valoración de riesgos[4]	Verificar que los riesgos considerados sean reales. Verificar si la valoración ha sido realizada o auditada por un ente externo independiente y calificado.
Estructura del proceso de valoración de riesgos	Verificar que riesgos relevantes no hayan sido omitidos. Verificar la valoración adecuada de los riesgos. Verificar si existe un plan de monitoreo de la valoración de riesgos.

[4] Risk Management Guide for information Technology Systems, Special Publication 800-30, Recommendations of the National Institute of Standards and Technology, October 2001.
HANDBOOK 3, RISK MANAGEMENT, Version 1.0, Australian Communications - Electronic Security Instruction 33 (ACSI 33).

2.3 REQUISITO PS03 –CONTINUIDAD DEL NEGOCIO Y RECUPERACION DE DESASTRES

2.3.1 ESPECIFICACIONES

Nombre	Continuidad del Negocio y Recuperación de Desastres.
Objetivo	Verificar el PLAN DE CONTINUIDAD DEL NEGOCIO y el PLAN DE RECUPERACIÓN DE DESASTRES establecidos para reducir a un nivel mínimo el efecto de interrupciones y/o alteraciones del servicio del PSC, mediante una combinación de planes preventivos y planes de contingencia.
Descripción	El Plan de Continuidad del Negocio y el Plan de Recuperación de Desastres, debe describir cómo los servicios serán afectados y posteriormente restaurados en el eventual caso de desastres, una caída de los sistemas, fallas de seguridad u otra anomalía. Se debería implantar un proceso de gestión de continuidad del negocio para reducir, a niveles aceptables, la interrupción causada por los desastres y fallas de seguridad (que puedan resultar; por ejemplo, de desastres naturales, accidentes, fallas de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación. Este proceso debe identificar los procesos críticos de negocio e integrar los requisitos de gestión de la seguridad de información para la continuidad del negocio con otros requisitos de continuidad relacionados con dichos aspectos como operaciones, proveedores de personal, materiales, transporte e instalaciones. Se deben desarrollar planes de mantenimiento y recuperación de las operaciones del negocio, para asegurar la disponibilidad de información al nivel y en las escalas de tiempo requeridas, tras la interrupción o la falla de sus procesos críticos. También se deberá especificar un Análisis de Impacto en los Negocios, siendo esta una evaluación y tratamiento del efecto de las interrupciones no planificadas en el negocio. El plan deberá además incluir mecanismos para la preservación de evidencia de mal uso de los sistemas, cuyo propósito es proporcionar evidencia admisible en una corte judicial en alguna fecha posterior.

Dependencias	PS02 - Revisión de Análisis de Riesgos y Amenazas.
Estándares de evaluación	NTP-ISO/IEC 17799, BS 7799-II, ISO IEC 27001, ETSI TI 102 042
Documentación solicitada	Plan de Continuidad del Negocio Plan de Recuperación de Desastres
Evidencias solicitadas	Ninguna

2.3.2 ASPECTOS/CONTROLES ESPECÍFICOS A EVALUAR

Aspectos/Controles	Evaluación
Conformidad con el estándar NTP-ISO/IEC 17799 sección 14.1.3 ISO 27001 sección 14.1.3	Verificar que los requerimientos de la sección 14.1.3 del anexo 5 de la Guía de Acreditación de EC, están incorporados.
Conformidad con el estándar NTP-ISO/IEC 17799 sección 14.1.5 ISO 27001 sección 14.1.5	Verificar que se ha incluido un procedimiento de pruebas, mantenimiento y evaluación periódica de la Política de Seguridad.
Conformidad con el estándar ETSI TI 102 042 sección 7.4.8	Verificar que el plan incorpora procedimientos especialmente detallados para el caso de compromiso de la clave privada de firma tal como lo indica el estándar ETSI.
Viabilidad de las facilidades computacionales	Verificar que las facilidades computacionales alternativas consideradas en el plan, cumplen con los requerimientos mínimos para la operación del PSC.
Elementos de auditoría	Verificar que el sistema en el cual el PSC basa sus servicios provee mecanismos de preservación de los elementos de auditoría.

2.4 REQUISITO PS04 – DOCUMENTACIÓN, MANTENIMIENTO Y PLANIFICACIÓN DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN Y ADMINISTRACIÓN DE CLAVES

2.4.1 ESPECIFICACIONES

Nombre	Documentación, Mantenimiento y Planificación de Seguridad de Seguridad de Sistemas de Información y Administración de claves.
Objetivo	Verificar que el PSC tiene un plan para la seguridad del sistema de información y administración de claves coherente con su POLÍTICA DE SEGURIDAD.
Descripción	El Plan de Seguridad del Sistemas de Información y administración de Claves deberá describir las acciones operacionales, procedimientos y mecanismos que permitan lograr los objetivos indicados en la Política de Seguridad del PSC. Las claves criptográficas son la base de la IOFE, siendo el elemento principal a proteger y administrar por el PSC, por lo que requiere de un plan específico para su administración. El plan de Administración de Claves deberá contemplar la protección de todos los tipos de claves, su modificación o destrucción. Las claves secretas y las privadas requieren protección contra su distribución no autorizada, para lo cual pueden usarse técnicas criptográficas, además se debería utilizar protección física para cubrir el equipo usado en la generación, almacenamiento y archivo de claves. El sistema de gestión de claves se debe basar en un conjunto acordado de normas, procedimientos y métodos seguros. El plan de seguridad tendrá que considerar a lo menos las secciones 5 al 14 del estándar NTP-ISO/IEC 17799 o según ISO 27001, presentado en el anexo 5. Sin embargo, en este requisito se evaluarán en particular los siguientes aspectos: • Seguridad Organizacional. • Control y Clasificación de activos. • Gestión de las Comunicaciones y Operaciones. • Control de accesos. • Adquisición, Desarrollo y Mantenimiento de sistemas.
Dependencias	PS02

Estándares de evaluación	NTP-ISO/IEC 17799, BS 7799-II, ISO IEC 27001.
Documentación solicitada	Plan de Seguridad del Sistema Información. Plan de Administración de claves.
Evidencias Solicitadas	Ninguna

2.4.2 ASPECTOS/CONTROLES ESPECÍFICOS A EVALUAR

Aspectos/Controles	**Evaluación**
Relación entre Plan de Seguridad y Valoración de Riesgos	Verificar que los procedimientos y mecanismos de seguridad permitan identificar el riesgo residual determinado en la Valoración de Riesgos.
Relación entre Plan de Seguridad y Política de Seguridad	Verificar que los procedimientos y mecanismos del Plan se Seguridad del Sistema de Información permitan lograr los objetivos de la Política de Seguridad.
Plan de Seguridad perdurable	Verificar que el Plan de Seguridad incluye los procedimientos necesarios para lograr que la seguridad del PSC perdure en el tiempo ante cambios o riesgos en: personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Seguridad con las prácticas y Política General de certificación	Verificar que los objetivos de seguridad enunciados en la CPS y la CP se logran a través del Plan de Seguridad del Sistema de Información.
Requerimientos ISO NTP-ISO/IEC 17799, sección 6 **ISO 27001 sección 6**	Verificar que los controles de Aspectos Organizativos para la Seguridad del estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de esta Guía).
Requerimientos NTP-ISO/IEC 17799, sección 7 **ISO 27001 sección 7**	Verificar que los controles de Clasificación y Control de Activos del estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de la Guía de Acreditación de EC).

Requerimientos NTP-ISO/IEC 17799, sección 8 **ISO 27001 sección 8**	Verificar que los controles de Seguridad en Recursos Humanos del estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de la Guía de Acreditación de EC).
Requerimientos NTP-ISO/IEC 17799, sección 9 **ISO 27001 sección 9**	Verificar que los controles de Seguridad Física y del Entorno del estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de la Guía de Acreditación de EC).
Requerimientos NTP-ISO/IEC 17799, sección 10 **ISO 27001 sección 10**	Verificar que los controles de Gestión de Comunicaciones y Operaciones del estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de la Guía de Acreditación de EC).
Requerimientos NTP-ISO/IEC 17799, sección 11 **ISO 27001 sección 11**	Verificar que los controles de Controles de Accesos del estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de la Guía de Acreditación de EC).
Requerimientos NTP-ISO/EIC 17799, sección 12 **ISO 27001 sección 12**	Verificar que los controles de Adquisición, Desarrollo y Mantenimiento de Sistemas del estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de la Guía de Acreditación de EC).
Administración de claves criptográficas **NTP-ISO/EIC 17799, sección 12.3.2** **ISO 27001 sección 12.3.2** **ETSI TS 102 042 sección 7.2**	Verificar que el Plan de Administración de Claves Criptográficas cubre todo el ciclo de vida de estas claves.

Destrucción de claves criptográficas NTP-ISO/EIC 17799, sección 12.3.2 **ISO 27001 sección 12.3.2** **ETSI TS 102 042 Sección 7.2.6**	Verificar que el Plan de Administración de Claves Criptográficas contemple la destrucción de las claves criptográficas al finalizar el ciclo de vida de estas claves.
Protección del repositorio de acceso público **NTP-ISO/EIC 17799, sección 12.3.2** **ISO 27001 sección 12.3.2**	Verificar que el Plan de Seguridad del Sistema de Información contiene medidas especiales de protección del repositorio público de certificados.
Gestión de Incidentes en la Seguridad de la Información **NTP-ISO/EIC 17799, sección 13** **ISO 27001 sección 13**	Verificar que el Plan de Seguridad del Sistema de Información contiene medidas para la gestión de eventos, incidentes y debilidades de la seguridad de la información.
Gestión de mejoras en la seguridad de la información **NTP-ISO/EIC 17799, sección 13.2** **ISO 27001 sección 13.2**	Verificar que el Plan de Seguridad del Sistema de Información contiene medidas para la gestión de las mejoras de la seguridad de la información.

Protección de información privada **NTP-ISO/EIC 17799** **sección 6.1.5** **sección 6.2.2** **sección 15.1.4** **ISO 27001** **sección 6.1.5** **sección 6.2.2** **sección 15.1.4**	Verificar que el Plan de Seguridad del Sistema de Información incluye medidas de protección para información privada e información confidencial; y que además cumple con los lineamientos del APEC.

2.5 REQUISITO PS05 – EVALUACIÓN DE LA IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN

2.5.1 ESPECIFICACIONES

Nombre	Evaluación de la Implementación del Plan de Seguridad del Sistema de Información.
Objetivo	Verificar y comprobar que el PSC tiene implementado un Plan de Seguridad del Sistema de Información coherente con su POLÍTICA DE SEGURIDAD, de modo que se pueda mostrar un nivel de confianza acorde con lo planificado.
Descripción	El PSC deberá mostrar sus procedimientos de implementación de la seguridad del sistema de información de acuerdo con el Plan de Seguridad del Sistema de Información, dichos procedimientos deben contener lo siguiente: o Acciones, procedimientos y mecanismos documentados que permiten lograr los objetivos indicados en el Plan de Seguridad del PSC. o Que estos controles sean coherentes con los requerimientos del estándar NTP-ISO/IEC 17799 o ISO 27001, en particular los correspondientes a los siguientes aspectos: • Aspectos Organizativos para la Seguridad. • Clasificación y Control de Activos. • Seguridad en Recursos Humanos. • Seguridad Física y del Entorno. • Gestión de Comunicaciones y Operaciones. • Controles de Accesos. • Adquisición, Desarrollo y Mantenimiento de Sistemas.
Dependencias	PS03, PS04 y ET01.
Estándares de evaluación	NTP-ISO/IEC 17799, BS 7799-II, ISO IEC 27001.
Documentación solicitada	Ninguna.
Evidencias solicitadas	Informe de la Auditoría realizada en las instalaciones del PSC por un auditor independiente.

2.5.2 ASPECTOS/CONTROLES ESPECÍFICOS A EVALUAR

Aspectos/Controles	Evaluación
Relación entre el Plan de Seguridad del Sistema de Información[5] y los recursos asignados NIST SP800-18 NIST SP800-26	Verificar que el PSC dispone de los recursos y capacidades para implementar los mecanismos y procedimientos de seguridad.
Relación entre Plan de Seguridad del Sistema de Información y Política de Seguridad	Verificar que los procedimientos, acciones y mecanismos de seguridad implementados permiten alcanzar y verificar los objetivos de la Política de Seguridad.
Plan de Seguridad	Verificar que el Plan de Seguridad del Sistema de Información incluye los procedimientos necesarios para lograr que la seguridad del PSC perdure en el tiempo ante cambios o riesgos en: personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Seguridad con las prácticas y la Política General de certificación	Verificar que los objetivos de seguridad enunciados en la CPS y la Política General de Certificación se logran a través del Plan de Seguridad del Sistema de Información.
Requerimientos ISO NTP-ISO/IEC 17799, sección 6 ISO 27001 sección 6	Verificar que los controles de Aspectos Organizativos para la Seguridad contemplados en la sección 6 del estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de la Guía de Acreditación de EC).
Requerimientos NTP-ISO/IEC 17799, sección 7 ISO 27001 sección 7	Verificar que los controles de Clasificación y Control de Activos contemplados en la sección 7 del estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de la Guía de Acreditación de EC).

[5] NIST SP800-18, Guide for Developing Security Plans for Information Technology Systems.
NIST SP800-26 Self Assessment Guide IT Systems Review.

Requerimientos NTP-ISO/IEC 17799, sección 8 **ISO 27001 sección 8**	Verificar que los controles de Seguridad en Recursos Humanos contemplados en la sección 8 del estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de la Guía de Acreditación de EC).
Requerimientos NTP-ISO/IEC 17799, sección 9 **ISO 27001 sección 9**	Verificar que los controles de Seguridad Física y del Entorno del contemplados en la sección 9 estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de esta de Guía).
Requerimientos NTP-ISO/IEC 17799, sección 10 **ISO 27001 sección 10**	Verificar que los controles de Gestión de Comunicaciones y Operaciones contemplados en la sección 10 del estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de la Guía de Acreditación de EC).
Requerimientos NTP-ISO/IEC 17799, sección 11 **ISO 27001 sección 11**	Verificar que los controles de Controles de Accesos contemplados en la sección 11 del estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de la Guía de Acreditación de EC).
Requerimientos NTP-ISO/EIC 17799, sección 12 **ISO 27001 sección 12**	Verificar que los controles de Adquisición, Desarrollo y Mantenimiento de Sistemas contemplados en la sección 12 del estándar NTP-ISO/IEC 17799 o ISO 27001 están considerados (indicados en el anexo 5 de la Guía de Acreditación de EC).
Protección del repositorio de acceso público **NTP-ISO/EIC 17799, sección 12** **ISO 27001 sección 12**	Verificar que la implementación del Plan de Seguridad contiene medidas especiales de protección del repositorio público de certificados.
Protección de información privada **NTP-ISO/EIC 17799,** **sección 6.1.5** **sección 6.2.2** **sección 15.1.4** **ISO 27001,** **sección 6.1.5** **sección 6.2.2** **sección 15.1.4**	Verificar que la implementación del Plan de Seguridad incluye medidas de protección de la información privada e información confidencial y además cumple con los lineamientos del APEC.

2.6 REQUISITO PS06 – EVALUACIÓN DEL PLAN DE ADMINISTRACIÓN DE CLAVES

2.6.1 ESPECIFICACIONES

Nombre	Evaluación del Plan de Administración de Claves.
Objetivo	Verificar que el PSC tiene implementado un PLAN DE ADMINISTRACIÓN DE CLAVES coherente con su POLÍTICA DE SEGURIDAD, que permita mostrar un nivel de confianza acorde con lo planificado.
Descripción	El PSC deberá mostrar sus procedimientos de administración de la claves criptográficas y la capacidad de administrar estas de acuerdo con el PLAN DE ADMINISTRACIÓN DE CLAVES, este documento deberá contener: • Documentación del ciclo de vida completo de las claves criptográficas, esto es: o Generación. o Almacenamiento, respaldo y recuperación (en el caso que corresponda). o Distribución de la clave pública. o Término del ciclo de vida de la EC (en el caso corresponda). • Destrucción de la clave privada. • Servicios de administración de las claves de los titulares suministradas por la EC. • Procedimientos de los dispositivos seguros de los usuarios.
Dependencias	PS02 y PS04
Estándares de evaluación	ETSI TS 102 042 y FIPS 140-2 Nivel de seguridad 3
Documentación solicitada	Ninguna.
Evidencias	Informe de Auditoría en las instalaciones del PSC realizadas por un auditor independiente

2.6.2 ASPECTOS/CONTROLES ESPECÍFICOS A EVALUAR

Aspectos/Controles	Evaluación
Relación entre el Plan de Administración de Claves y los recursos asignados	Verificar que el PSC dispone de los procedimientos y procesos adecuados para implementar el Plan de Administración de Claves.
Relación entre Plan de Administración de Claves y Valoración de riesgos	Verificar que los procedimientos y mecanismos de administración de claves implementados permiten determinar, evaluar los riesgos determinados en la Valoración de Riesgos.
Plan de Administración de Claves	Verificar que los procedimientos implementados de acuerdo al Plan de Administración de Claves posibilitan que la seguridad de las claves continúe en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Administración de Claves con la CP Y CPS	Verificar que los objetivos de seguridad enunciados en la CPS y la CP se logran a través de la implementación del Plan de Administración de Claves.
Requerimientos ETSI TS 102 042, sección 7.2.1	Verificar que los requerimientos de Generación de Claves de la EC, contemplados en la sección 7.2.1 del estándar ETSI TS 102 042 están considerados.
Requerimientos ETSI TS 102 042, sección 7.2.2	Verificar que los requerimientos de almacenamiento, respaldo y recuperación, contemplados en la sección 7.2.2 del estándar ETSI TS 102 042 están considerados.
Requerimientos ETSI TS 102 042, sección 7.2.3	Verificar que los requerimientos de distribución de la clave pública de la EC, contemplados en la sección 7.2.3 del estándar ETSI TS 102 042 están considerados.
Requerimientos ETSI TS 102 042, sección 7.2.5	Verificar que los requerimientos de uso de clave de la EC, contemplados en la sección 7.2.5 del estándar ETSI TS 102 042 están considerados.
Requerimientos ETSI TS 102 042, sección 7.2.6	Verificar que los requerimientos de fin del ciclo de vida de la clave de la EC, contemplados en la sección 7.2.6 del estándar ETSI TS 102 042 están considerados.

Requerimientos ETSI TS 102 042, sección 7.2.7	Verificar que los requerimientos de administración del hardware criptográfico contemplados en la sección 7.2.7 del estándar ETSI TS 102 042 están considerados.
Nivel de seguridad del dispositivo de almacenamiento de los usuarios	Verificar que el dispositivo de almacenamiento seguro de los usuarios cumple como mínimo con los requerimientos del estándar FIPS 140-2 nivel de seguridad 3 en el caso de las ECs y FIPS 140-2 nivel de seguridad 2 en el caso de las ERs, en sus elementos de seguridad e implementación de los algoritmos criptográficos estándares.

2.7 REQUISITO CT01 – EVALUACIÓN Y CERTIFICACIÓN DE LA PLATAFORMA TECNOLÓGICA.

2.7.1 ESPECIFICACIONES

Nombre	Evaluación y certificación de la plataforma tecnológica.
Objetivo	Verificar y evaluar los elementos que la plataforma tecnológica utiliza para la generación, publicación y administración de certificados digitales y CRLs.
Descripción	Los elementos de la plataforma Tecnológica deben ser confiables; tanto los componentes de hardware como software, además de todos los elementos de apoyo y soporte. Los elementos a considerar son: • Módulo criptográfico. • Módulo EC (Entidad Certificadora). • Módulo ER (Entidad de Registro). • Módulo de Almacenamiento y Publicación de Certificados. • Protocolos de comunicación entre EC y ER. • Elementos de administración de logs y auditoria.
Dependencias	PS02 y PS03
Estándares de evaluación	NTP-ISO/IEC 17799, BS 7799-II, ISO IEC 27001, FIPS 140-2, ISO/IEC 15408 o equivalente.
Documentación solicitada	Documento de Cumplimiento de Estándares Tecnológicos. En este documento se debe especificar una lista detallada de dispositivos de seguridad, también debe contener detalles de los elementos que permitan asegurar la confiabilidad de la plataforma. Manuales de los fabricantes de los productos hardware y software presentes en la infraestructura.
Evidencias solicitadas	Informe Auditor Independiente que acredite el correspondiente nivel de seguridad correspondiente a cada elemento. Documento de Cumplimiento de Estándares Tecnológicos.

2.7.2 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto / Controles	Evaluación
Módulo criptográfico.	1. Funcionalidad y operación: • Generar pares de clave privada y pública con longitudes de al menos 1024 bits (CC P2 FCS_COP.1) y según los niveles de seguridad establecidos en la Guía de Acreditación EC (Nivel Medio y Medio Alto). Capacidad de firma, autenticación y cifrado (CC P2 FCS_CKM.2) 2. Seguridad. • Sistema control de acceso para acceder a la clave privada. • Control de acceso para acceder a funcionalidades de firma, autenticación y cifrado. 3. Ciclo de vida. • Capacidad de respaldar la clave privada, en forma segura. • Capacidad de recuperar la clave privada de back-up. 4. Auditoria. • Capacidad de generar un Log auditable para administración de contingencia y accesos maliciosos. 5. Documentación. • Manuales de operación, configuración y puesta en marcha. • Procedimiento de Recuperación ante contingencia. 6. Certificación Que cuente con la certificación FIPS – ISO 15408.

Módulo EC (Entidad Certificadora)	1. Funcionalidad y operación: • Capacidad para generar certificados con claves de al menos 1024 bits y según los niveles de seguridad establecidos en la Guía de Acreditación EC. • Capacidad para generar CRLs. • Capacidad de generar certificados de comunicación segura, entre EC y ER, si corresponde a la arquitectura (CC P2 FTP_ITC.1). • Capacidad de entregar certificados y CRLs a directorios públicos X.500. 2. Seguridad. • Existencia de sistema de control de acceso para acceder a la generación de certificados (CC P2 FIA_SOS.2). • Existencia de sistema de control de acceso para acceder a los sistemas de administración y auditoría (CC P2 FIA_UAU.2). 3. Ciclo de vida. • Capacidad de generación de certificados. • Capacidad de revocar certificados. • Capacidad de revocar certificado raíz y generar uno nuevo según lo establezca la EC. • Capacidad de suspender, modificar o re-emitir certificados. • Capacidad de destruir certificados. 4. Auditoria. • Capacidad de generar Log auditable para administración de contingencia, actividades diarias del personal autorizado y accesos maliciosos (CC P2 FAU_STG.2). 5. Documentación. • Manuales de operación, configuración y puesta en marcha. • Procedimiento de Recuperación de Desastres y Plan de Contingencias.

Módulo de ER (Entidad de Registro)	1.- Funcionalidad y operación: • Capacidad de recibir requerimientos de certificados (CC P2 FCS_CKM.2). • Autorizar la solicitud emisión de certificado a la EC. 2.- Seguridad. • Existencia de sistema de control de acceso para acceder a la generación de certificados. • Existencia de sistema de control de acceso para acceder a los sistemas de administración y auditoria. 3.- Ciclo de vida. • Capacidad de autorizar las solicitudes de emisión y revocación de certificado. • Capacidad para autorizar las solicitudes de suspensión, modificación y re-emisión de certificados, según lo establezca la EC. 4.- Auditoria. • Capacidad de generar un Log auditable para administración de contingencia y accesos maliciosos. 5.- Documentación. • Manuales de operación, configuración y puesta en marcha. • Política de Seguridad ER, conforme a lo establecido en la Guía de Acreditación ER.
Protocolos de comunicación entre ER y EC	Capacidad de generar certificados de comunicación segura, entre EC y ER, si corresponde a la arquitectura, utilizando un protocolo estándar de la industria (CC P2 FTP_ITC.1).
Elementos de administración de Log y auditoria	Debe existir módulos de Log y de auditoría, que permitan verificar los intentos de acceso, los accesos y las operaciones dañinas, sean esta intencionadas o no.

2.8 REQUISITO SF01 – SEGURIDAD FÍSICA Y AMBIENTAL DE LA INFRAESTRUCTURA DEL PSC

2.8.1 ESPECIFICACIONES

Nombre	Seguridad física y ambiental de la infraestructura del PSC
Objetivo	Planificar y evaluar los requerimientos relacionados con el aseguramiento de áreas restringidas, equipos e información bajo el marco de un PLAN DE SEGURIDAD FÍSICA Y AMBIENTAL.
Descripción	El PSC debe minimizar la ocurrencia de los accesos no autorizados, daños e interferencias contra los locales y la información de la organización. Los accesos físicos a las siguientes áreas restringidas deben ser otorgadas solo al personal autorizado previa identificación: • Generación de certificados. • Entrega de dispositivos seguros a titulares. • Servicios de gestión de revocación. • Área de servidores del PSC. Se debe dar protección física contra accesos no autorizados, daños e interferencias, dicha protección debe ser proporcional a los riesgos identificados. En lo concerniente a los sistemas de generación de certificados así como a los elementos que lo soportan y apoyan se debe contemplar: • Controles físico de acceso • Protección y recuperación ante desastres naturales • Protección contra robos, forzamiento • Medidas de protección en caso de incendios • Medidas de protección en servicio. • Medidas ante falla de servicios de soporte (electricidad, telecomunicaciones, etc.) • Medidas en caso de fallas estructurales o de humedad en las redes. • Servicio técnico para los servicios básicos

Dependencias	PS04
Estándares de evaluación	ETSI 102 042 V1.1.1 (2002-4), 7.4.4 Physical and environment security. NTP-ISO/IEC 17799, BS 7799-II, ISO IEC 27001.
Documentación solicitada	Plan de Seguridad Física y Ambiental.
Evidencias solicitadas	Informe Auditor Independiente como resultado de la evaluación en las instalaciones del PSC por auditor independiente.

2.8.2 ASPECTOS/CONTROLES ESPECÍFICOS A EVALUAR

Aspectos / controles	Evaluación
Perímetro de Seguridad Física NTC-ISO/IEC 17799, sección 9.1.1 ISO 27001, sección 9.1.1	Verificar que exista un perímetro de seguridad, el cual debe estar claramente definido y el lugar y fuerza de cada perímetro debe depender de los requerimientos de seguridad del activo entre el perímetro y los resultados de la evaluación de riesgos. El perímetro de un edificio o un lugar que contenga recursos de tratamiento de información debería tener solidez física. Verificar que las áreas donde se ubican los sistemas implicados en el ciclo de vida de los certificados (generación, revocación, etc.) estén debidamente protegidos mediante puertas y paredes firmes, chapas seguras, controles de acceso, y alarmas de seguridad e incendio. Verificar la instalación de sistemas adecuados de detección de intrusos de acuerdo a estándares regionales, nacionales o internacionales y deben ser regularmente probados para cubrir todas las puertas externas y ventanas de acceso.
Controles físicos de entrada NTC-ISO/IEC 17799, sección 9.1.2 ISO 27001, sección 9.1.2	Verificar que las visitas a las áreas seguras sean supervisadas, a menos que el acceso haya sido aprobado previamente, y se registre la fecha y momento de entrada y salida. Los visitantes sólo tendrán acceso para propósitos específicos y autorizados, proporcionándoles instrucciones sobre los requisitos de seguridad del área y los procedimientos de emergencia; se debe exigir a todo el personal que lleve puesta alguna forma de identificación visible y se le pedirá que solicite a los extraños no acompañados y a cualquiera que no lleve dicha identificación visible, que se identifique; se debe garantizar el acceso restringido al personal de apoyo de terceros, hacia áreas de seguridad o a los recursos de procesamiento de información sensibles, solo cuando este sea requerido. Este acceso debe ser autorizado y supervisado

	Verificar que los visitantes deben estar claramente identificados en todo momento con una credencial visible mientras se encuentren dentro del perímetro y su acceso solo debe permitirse para propósitos específicos. Las actividades de los visitantes, la hora y fecha de su ingreso y salida deben ser registradas.
Seguridad de oficinas, salas y servicios básico **NTP-ISO/IEC 17799, sección 9.1.3** **sección 9.1.4** **ISO 27001, sección 9.1.3** **sección 9.1.4**	Verificar que los servicios claves deben situarse en lugares alejados del acceso o atención de público. Verificar que el material impreso en desuso, debe ser destruido de tal modo que se imposibilite la recuperación después de ser destruido. Verificar que los materiales peligrosos y combustibles se deben almacenar en algún lugar distante de las áreas seguras. No se deben almacenar dentro de un área segura suministros hasta que se necesiten. El equipo y los medios de respaldo deben estar a una distancia de seguridad conveniente para evitar que se dañen por un desastre en el área principal. Verificar que sean consideradas las regulaciones y estándares de salud y seguridad. Verificar que se debe implementar seguridad física para oficinas, despachos y recursos. Las áreas seguras como oficinas y salas deberán estar cerradas y contener gabinetes cerrados y seguros Para seleccionar un área segura se deben consideran medidas que prevengan el daño por fuego, fluidos, desordenes civiles, desastres naturales o provocados por el hombre.
Trabajo en áreas seguras **NTP-ISO/IEC 17799, sección 9.1.5** **ISO 27001, sección 9.1.5**	Verificar el diseño e implementación de protección física y normas para trabajar en áreas seguras, para lo cual se debe considerar: - El personal debe conocer los procedimientos y practicas necesarias para garantizar la seguridad dentro de un área segura. - Evitar el trabajo no supervisado en áreas seguras tanto por motivos de salud como para evitar oportunidades de actividades maliciosas. - Las áreas vacías deben ser bloqueadas y revisadas periódicamente.

	- El personal de servicios de soporte que no pertenece al personal de la EC, sólo debe poder acceder a las áreas restringidas en caso de ser necesario, e l acceso de este personal debe ser previamente autorizado, registrado y monitoreado. - No se debe permitir ningún tipo de grabación o filmación visual o auditiva al interior de las áreas seguras.
Áreas de Acceso al Publico **NTP-ISO/IEC 17799, sección 9.1.6** **ISO 27001, sección 9.1.6**	Verificar que se deben controlar las áreas de carga y descarga; y si es posible se deben aislar los recursos de tratamiento de información para evitar accesos no autorizados. Verificar que las áreas de carga, descarga y salida de basura o cualquier elemento de desecho producido como parte de la operación sean controladas y separadas del área de procesamiento de la información para evitar el acceso no autorizado. Verificar que los requerimientos de seguridad para las áreas de atención al cliente deben ser determinados a partir de una evaluación de riesgos. Verificar que el personal que acceda a las áreas externas de la recepción de insumos y entrega de materiales o desechos esté debidamente controlado. Verificar que el personal no autorizado, no pueda acceder a través de estas áreas a los perímetros definidos de seguridad. Verificar que las puertas externas de las áreas mencionadas estén aseguradas cuando las puertas internas se encuentren abiertas. Verificar que se debe registrar el material entrante, en concordancia con los procedimientos de gestión de activos al entrar en el perímetro de seguridad.
Resguardo y protección del equipamiento **NTP-ISO/IEC 17799, sección 9.2.1** **ISO 27001, sección 9.2.1**	Verificar que los equipos de tratamiento de información deben situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. Verificar que la EC debe incluir en su Política de Seguridad cuestiones sobre fumar, beber y/o comer cerca de los equipos de tratamiento de información. Verificar la vigilancia de las condiciones ambientales, como temperatura y humedad para impedir , que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información

Suministro Eléctrico **NTP-ISO/IEC 17799, sección 9.2.2** **ISO 27001, sección 9.2.2**	Verificar que los equipos deben ser protegidos contra fallos de energía u otras anomalías eléctricas. Verificar la instalación de un Sistema de Alimentación Ininterrumpida (U.P.S.). Se deben cubrir mediante planes de contingencia las acciones a adoptar en caso de fallo del UPS. Si un proceso debe continuar en caso de fallo prolongado de energía, se debe instalar un generador de respaldo, en este caso se deben hacer pruebas y simulacros regularmente de acuerdo con las recomendaciones del fabricante. Verificar que se debe disponer de una reserva suficiente de combustible para asegurar el funcionamiento del generador durante un periodo prolongado. Los equipos de UPS y los generadores se deben revisar regularmente para asegurar que tienen la capacidad adecuada y deben ser probados de acuerdo con las recomendaciones del fabricante. En adición, se pueden dar consideraciones para el uso de múltiples fuentes de poder, si el lugar es amplio, una subestación de poder separada
Seguridad del cableado **NTP-ISO/IEC 17799, sección 9.2.3** **ISO 27001, sección 9.2.3**	Verificar que se debe proteger contra interceptaciones o daños el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información. Verificar que se debe proteger la red cableada contra intercepciones no autorizadas o daños, por ejemplo, usando conductos y evitando rutas a través de áreas públicas. Verificar la separación de los cables de energía de los de comunicaciones para evitar interferencias electromagnéticas que ocasionen pérdida de datos u otros riesgos. Los cables deben estar claramente identificados y marcados con el fin de minimizar errores de manejo.
Mantenimiento de equipos. **NTP-ISO/IEC 17799, sección 9.2.4** **ISO 27001, sección 9.2.4**	Verificar que sólo el personal autorizado debe tener acceso al mantenimiento de equipos. Los equipos se deben operar de manera correcta de acuerdo a las recomendaciones de intervalos y especificaciones del proveedor del producto; para asegurar su continua disponibilidad e integridad. Se deben documentar todo tipo de procedimientos e incidentes que ocurran antes, durante y después del proceso de mantenimiento. Se deben implementar medidas de seguridad apropiadas cuando el equipo es programado para mantenimiento.

Seguridad del equipamiento portátil **NTP-ISO/IEC 17799, sección 9.2.5** **ISO 27001, sección 9.2.5**	Verificar que existan procedimientos y prácticas de monitoreo y registro que eviten que ningún equipo portátil contenga información sensible. Si existieran por alguna razón justificada equipos portátiles que contengan información o procesos críticos de la operación del PSC o información privada de los titulares de los certificados, nunca salgan del perímetro de seguridad designado para ellos.
Seguridad la reutilización o eliminación del equipo **NTP-ISO/IEC 17799, sección 9.2.6** **ISO 27001, sección 9.2.6** **ISO 27001, sección 9.2.6**	Verificar que los medios de almacenamiento magnético u óptico que dejen de prestar servicio dentro de los perímetros de seguridad deben ser monitoreados y registrados durante el proceso de formateo para posteriormente ser destruidos antes de salir del perímetro. Los dispositivos dañados que contienen información sensible (por ejemplo el caso de la clave privada) pueden requerir una evaluación de riesgos para determinar si es que deben ser destruidos físicamente en lugar de ser reparados o descartados.
Seguridad en el equipo de escritorio **NTP-ISO/IEC 17799, sección 9.2.6** **ISO 27001, sección**	Verificar la adopción de la política de “escritorio limpio” y “pantalla limpia” como práctica conocida que permita reducir los riesgos de acceso no autorizado, perdidas o daños de la información durante o fuera el horario normal de trabajo.
Retiro de la propiedad **NTP-ISO/IEC 17799, sección 9.2.7** **ISO 27001, sección 9.2.7**	Verificar que existen procedimientos para evitar que el equipo, información o software pueda ser sacado fuera del local sin autorización. Deben existir procedimientos y practicas para definir claramente al personal con autoridad para permitir el retiro de la propiedad de los activos, ya sea el caso de un empleado, contratista y tercero, cualquiera sea el caso deben ser identificados, supervisados y registrados.

2.9 REQUISITO RP01 – EVALUACION COMPLETA DE LOS PERFILES DEL PERSONAL A NIVEL ALTAMENTE CONFIABLE

2.9.1 ESPECIFICACIONES

Nombre	Evaluación completa de los perfiles del personal a nivel altamente confiable
Objetivo	Verificar que los empleados, contratistas y terceros cumplan con el perfil de sus puestos, entiendan sus responsabilidades para los que han sido considerados, reduciendo el riesgo de hurto, fraude o mal uso de las instalaciones.
Descripción	Se evaluará el procedimiento que utiliza el PSC para reclutar, seleccionar, evaluar y contratar personal crítico. Se evaluará el procedimiento que utiliza el PSC para comprobar los antecedentes del personal crítico antes de contratarlo y el procedimiento para chequear antecedentes del personal contratado. El personal de operaciones y sistemas no deben tener acceso a funciones de confianza, hasta que todos sus antecedentes sean razonablemente verificados. El personal que maneje información sensible, deber ser personal de planta. Deben existir contratos de confidencialidad que se extiendan mas allá de la vigencia del contrato del empleado y/o empresa externa. Se evaluará al personal (empleados, contratistas y terceros) bajo las siguientes condiciones: a) Que tenga la calificación técnica o profesional requerida para el cargo o función que desempeña. b) Que tenga la experiencia mínima requerida para el cargo y función que desempeña. c) Que no pose a antecedentes crediticios ni penales, policiales que lo inhabiliten. d) Que esté instruido en los procedimientos mínimos de seguridad que debe guardar en su función. e) Haber firmado un acuerdo de confidencialidad
Dependencias	PS02
Estándares de evaluación	NTP-ISO/IEC 17799, BS 7799-II, ISO IEC 27001.

Documentación solicitada	Documentación de evaluación del personal La documentación de evaluación del personal contiene lo siguiente: • Perfiles del personal que ocupa los cargos que manejan información sensible. • Currículum del personal que ocupan los cargos que manejan información sensible. • Procedimientos de verificación en la contratación y seguimiento de los antecedentes comerciales y penales del personal de la empresa.
Evidencias solicitadas	Informe de auditoria realizada en las instalaciones del PSC por auditor independiente.

2.9.2 ASPECTOS/CONTROLES ESPECÍFICOS A EVALUAR

Aspectos/Controles	Evaluación
Procedimiento de contratación del personal crítico	Evaluar el procedimiento definido por el PSC para la contratación del personal crítico.
Procedimiento de verificación de antecedentes del	Evaluar el procedimiento definido por el PSC para comprobar los antecedentes del personal crítico una vez seleccionado.
Antecedentes profesionales del personal crítico	Verificar las certificaciones académicas y profesionales del personal crítico que trabaja para el PSC, verificando la concordancia de los perfiles en cada cargo y función, con el análisis de riesgos.
Antecedentes crediticios del personal crítico	Verificar los antecedentes crediticios del personal critico que trabaja para el PSC.
Capacitación del personal crítico en aspectos de seguridad acorde a su función y cargo	Verificar que todo el personal de la organización y si es relevante, contratistas y usuarios de terceros deban recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales para la función de su trabajo.

Documentación solicitada	Documento de Evaluación del Oficial de Seguridad, el cual comprende lo siguiente: o Documentos que acrediten el perfil profesional emitidos por entidades reconocidas u homologadas por el Ministerio de Educación o bien por referentes de la industria. o Certificado de antecedentes comerciales. o Certificado de antecedentes penales. o Entrevista con el Oficial de Seguridad.
Evidencias solicitadas	Informe Auditor Independiente.

2.10 REQUISITO RP02 – EVALUACION DEL OFICIAL DE SEGURIDAD DE LA INSTALACION

2.10.1 ESPECIFICACIONES

Nombre	Evaluación del Oficial de Seguridad de la instalación (IT security manager).
Objetivo	Verificar la capacidad técnica, el perfil profesional y los antecedentes del Oficial de Seguridad empleado por el PSC.
Descripción	El Oficial de Seguridad es la persona encargada de velar por el cumplimiento de todos los procedimientos y prácticas de seguridad establecidas en las instalaciones del PSC. Los procedimientos de reclutamiento, evaluación, selección, y verificación de antecedentes penales del Oficial de Seguridad deben cumplir con un alto estándar de exigencia. En particular se debe comprobar que el Oficial de Seguridad cumpla los siguientes requisitos mínimos: a) El perfil recomendado como mínimo es Ingeniero Electrónico o equivalente con certificación y/o experiencia de al menos 5 años en el ámbito de la seguridad informática. b) Que no posea antecedentes crediticios ni penales que lo inhabiliten c) Haber firmado un acuerdo de confidencialidad. Adicionalmente se evaluaran las cláusulas contractuales, de modo que aseguren que la vigencia de los compromisos de no divulgación de información va mas allá de la vigencia de los contratos, en caso de cese del profesional en el cargo.
Dependencias	PS02
Estándares de evaluación	NTP-ISO/IEC 17799, BS 7799-II, ISO IEC 27001.
Documentación solicitada	Documento de Evaluación del Oficial de Seguridad Currículum del Oficial de Seguridad. Procedimientos del PSC aplicado en la contratación del Oficial de Seguridad. Comprobación de antecedentes penales. Acuerdo de Confidencialidad.

Evidencias solicitadas	Informe de auditor sobre: a) Documentos que acrediten el perfil profesional emitidos por entidades reconocidas u homologadas por el Ministerio de Educación o por referentes de la industria. b) Certificado de antecedentes penales. c) Entrevista con el Oficial de Seguridad.

2.10.2 ASPECTOS/CONTROLES ESPECÍFICOS A EVALUAR

Aspectos/Controles	Evaluación
Perfil del OS	Verificar el perfil exigido por el PSC
Procedimiento de contratación del OS	Evaluar el procedimiento definido por el PSC para la contratación del OS.
Procedimiento de verificación de antecedentes del OS	Evaluar el procedimiento definido por el PSC para comprobar los antecedentes del OS una vez seleccionado.
Antecedentes profesionales del OS	Verificar los antecedentes profesionales y curriculares del OS presentados por el PSC.
Antecedentes penales del OS	Verificar los antecedentes penales del OS.
Antecedentes crediticios del OS	Verificar los antecedentes crediticios del OS.