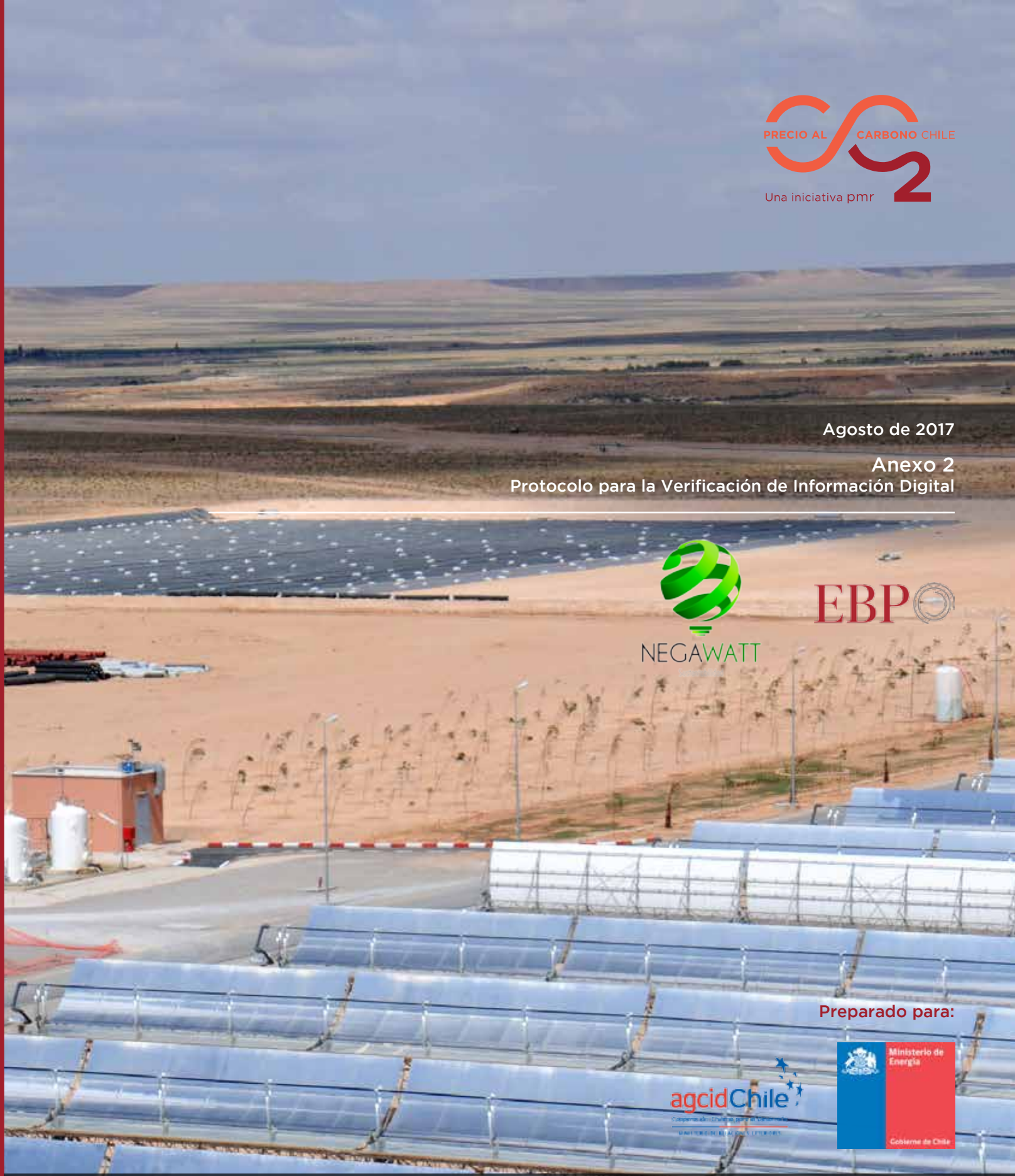
PRECIO AL CARBONO CHILE

Una iniciativa pmr

Agosto de 2017

Anexo 2
Protocolo para la Verificación de Información Digital



Preparado para:

Ministerio de Energía
Gobierno de Chile

Este estudio fue encargado por el proyecto Precio al Carbono Chile, parte de la iniciativa Partnership for Market Readiness del Banco Mundial cuya implementación se realiza en conjunto por el Ministerio de Energía (punto focal) y el Ministerio del Medio Ambiente. Los resultados del estudio forman parte de un conjunto de insumos para potenciales propuestas de fijación de precios al carbono en las que el proyecto está involucrado actualmente. La responsabilidad exclusiva de las opiniones, interpretaciones o conclusiones contenidas reside en los autores y no necesariamente reflejan la opinión del Gobierno de Chile o del Banco Mundial.

pmr PARTNERSHIP FOR MARKET READINESS

Anexo 2: Protocolo para la Verificación de Información Digital

11 de agosto de 2017

Paseo Bulnes 216, oficina 604 Santiago, Chile

Tabla de contenido

1. RESUMEN EJECUTIVO

Según lo acordado en reunión del día 23 de mayo en la SMA el entregable 'Protocolo de verificación de información digital' se modificó por un informe que contenga un resumen priorizado de las recomendaciones contenidas en dos guías del Banco Mundial y el informe final de la Consultoría realizada por DELOITTE en el marco del proyecto PMR-Chile.

De esta manera, el presente informe resume las recomendaciones contenidas en los siguientes documentos:

a. *Guide for designing mandatory greenhouse gas reporting programs, Banco Mundial (2015).*
b. *Building Systems for Corporate/Facility-Level Reporting, Banco Mundial (2016).*
c. *Informe de Diagnóstico de Ciberseguridad, Deloitte (2017).*

Adicionalmente, las recomendaciones generales extraídas de los documentos del Banco Mundial fueron linkeadas/aterrizadas al caso chileno y enriquecidas con la experiencia de las visitas a terreno y la revisión de experiencia internacional. Las principales recomendaciones para el caso chileno son:

- Respecto del sistema MR definido:
  - analizar la posibilidad de modificar la frecuencia trimestral de reporte actualmente vigente a una anual y exigir que el reporte de emisiones sea entregado junto con el informe de verificación en Enero o Febrero del año siguiente al período a reportar, de manera que la SMA alcance a revisar y entregar los datos a tiempo al SII.
  - estandarizar el contenido y nivel de detalle del Plan de Monitoreo que actualmente está contenido en la Metodología de medición presentada por el establecimiento y aprobada por la SMA.
  - analizar para una futura ampliación/modificación del impuesto verde la posibilidad de: a) incorporar la tasa de utilización (horas de operación anuales) de los equipos en el criterio de selección, b) modificar el criterio de selección por alguno de los sugeridos por el banco mundial, o c) incluir establecimientos que dada su potencia instalada y % de utilización de sus fuentes se estime emiten más que el establecimiento que menos reportó el año 2017.
- Respecto de la plataforma Impuesto Verde
  - implementar doble autenticación para envíos y cambios de información, y la diferenciación de perfiles por tipo de usuario (operacionales / gestores).
  - modificar el formato .csv, por otro estándar internacional que facilite el doble chequeo y sea de uso más conocido como .xls.
  - implementar funcionalidades para la validación de datos y verificación en línea.

Paseo Bulnes 216, oficina 604 Santiago, Chile

- implementar un canal confiable y expedito para recibir y dar respuesta oportuna a los establecimientos durante el período de reporte. Los plazos de respuesta deben ser conocidos y monitoreados, los usuarios deben poder hacer seguimiento a sus consultas y las preguntas frecuentes deben ser publicadas y actualizadas periódicamente.

2. ANTECEDENTES

Si bien de acuerdo a las Bases de Licitación se solicitó como entregable un 'Protocolo para la Verificación de Información Digital' que describiera las condiciones para cumplir estándares de aseguramiento de la calidad y control de calidad de la información reportada (QA & QC), en la reunión del día 23 de mayo en la SMA, según consta en la minuta respectiva, se acordó que el entregable 'Protocolo de verificación de información digital' consistiría en un resumen priorizado de las recomendaciones contenidas en dos guías del Banco Mundial que serían proporcionadas por la SMA al equipo consultor y el informe final de la Consultoría realizada por DELOITTE en el marco del proyecto PMR-Chile.

En la actualidad, más de 40 países a nivel mundial cuentan con sistemas de reporte obligatorio de emisiones. Una correcta gestión ambiental requiere de la disponibilidad de información precisa y de confianza para la toma de decisiones. Es en este contexto que el Grupo del Banco Mundial ha desarrollado una serie de guías con recomendaciones para facilitar los procesos de diseño e implementación de sistemas de reporte y a la vez maximizar las probabilidades de éxito de los mismos.

El capítulo 3 del presente informe resume las recomendaciones contenidas en los siguientes documentos:

a. World Bank Group. World Resources Institute (2015) *Guide for designing mandatory greenhouse gas reporting programs.*
b. World Bank Group (2016) *Greenhouse Gas Data Management. Building Systems for Corporate/Facility-Level Reporting.*

El primero pretende ser una guía para legisladores y profesionales a cargo del diseño de programas obligatorios para el reporte de emisiones de gases de efecto invernadero.

El segundo provee lineamientos para reguladores, administradores de sistemas y programas, y desarrolladores informáticos sobre cómo diseñar, desarrollar e implementar sistemas de manejo de datos de gases de efecto invernadero (GHG) para apoyar los programas de reporte a nivel de empresa y establecimiento. El documento se basó en la experiencia y lecciones aprendidas de 10 jurisdicciones alrededor del mundo y describe los procesos y consideraciones que pueden ayudar a los países a desarrollar soluciones a medida de sus propias necesidades, requerimientos, condiciones locales, política medioambiental y capacidad técnica, humana y financiera.

El capítulo 4 linkea las recomendaciones del Banco Mundial al caso chileno, considerando el sistema MR diseñado, la plataforma Impuesto Verde (SIV) implementado y las visitas a terreno.

Finalmente, el capítulo 5 contiene un resumen de las recomendaciones en el ámbito de ciberseguridad entregadas por Deloitte en el informe final de su Consultoría.

3. RECOMENDACIONES DEL BANCO MUNDIAL PARA EL DISEÑO DE UN PROGRAMA PARA EL REPORTE DE EMISIONES DE EFECTO INVERNADERO

Un paso fundamental en el diseño de un programa de reporte de emisiones es la determinación de requisitos básicos que aseguren la fiabilidad, consistencia, exactitud, transparencia e integridad de los datos. Se han definido 6 requisitos básicos:

1. Alcance del programa y objetivos
2. Metodologías para la cuantificación de emisiones para diferentes fuentes de emisiones y requisitos para el monitoreo de datos
3. Procedimientos para el reporte y definición de fechas claves
4. Plataformas para el reporte
5. Medidas de control y aseguramiento de la calidad
6. Medidas de coerción

3.1 Alcance del programa y objetivos

La definición del alcance y los objetivos del programa están dados por las respuestas a las siguientes preguntas:

a. ¿Quién reporta?

b. ¿Qué se reporta?

Para contestar la primera pregunta, se debe establecer claramente el nivel al cual será aplicable el sistema de reporte. ¿Será implementado a nivel de instalación (edificio o planta) o a nivel de empresa? En otras palabras, definir si el reporte está limitado o no, a uno o más espacios físicos determinados.

Así también, se debe definir si el reporte aplicará a emisiones directas o indirectas. Entendiendo por emisiones directas aquellas generadas a partir de fuentes que son de propiedad o que son controladas por el mismo agente emisor. En cuanto a las emisiones indirectas, estas se suelen clasificar en dos categorías:

i) aquellas emisiones que resultan por actividades del agente emisor generadas por fuentes que no son propiedad o que no son controladas por este, como es el caso de las emisiones generadas por el concepto de consumo eléctrico;

ii) aquellas emisiones generadas en la cadena de suministros del agente emisor, como por ejemplo emisiones generadas a partir de la compra de insumos, el transporte de materiales, etc.

Si la definición involucra ambos tipos de emisiones, directas e indirectas, estas se deben diferenciar claramente al momento del reporte a fin de evitar la doble contabilización de emisiones.

A continuación se deben definir criterios de aplicabilidad, es decir, bajo qué condiciones las instalaciones o compañías establecidas en el punto anterior deben hacer una declaración de emisiones. Algunos criterios de aplicabilidad son: tipo de fuente, número de empleados, toneladas de producción, consumo de energía y límite de emisiones, siendo este último el más utilizado en la actualidad.

Por último, se debe definir que emisiones serán reportadas. Esta definición está estrechamente ligada con los objetivos del programa. Algunos programas tienen su enfoque en las emisiones de efecto invernadero, mientras otros tienen un alcance mayor y cubren otras emisiones contaminantes. Otros factores que influyen en esta definición son los costos asociados a la medición, monitoreo y reporte de las emisiones seleccionadas, el presupuesto disponible, la cantidad de información generada, nivel de compromiso de las partes interesadas, requisitos tecnológicos, etc.

3.2 Metodologías para la cuantificación de emisiones para diferentes fuentes de emisiones y requisitos para el monitoreo de datos

El siguiente paso busca dar respuesta a la siguiente interrogante: ***¿Cómo medir y calcular las emisiones?*** De esta forma, se debe definir la metodología más apropiada para la medición o estimación de las emisiones previamente establecidas.

La cuantificación de emisiones puede ser realizado a través de dos enfoques no excluyentes: La medición directa de las emisiones o la estimación de estas en base a cálculos. La decisión sobre que enfoque utilizar va a depender de las características de la fuente de emisión. La definición de una metodología debe ser complementada con la entrega de información y asesoría respecto del enfoque:

Tabla 1. Enfoque utilizados en la cuantificación de emisiones

Medición Directa	Tipos de equipos de medición incluyendo softwares, certificación y calibración de equipos de medición, frecuencia de las mediciones, muestreo y registro de datos. Procedimientos para la sustitución de información faltante, otros.
Estimación en base cálculos	Determinación de factores de emisión e índice GWP, metodología de cálculo, nivel de incertidumbre, otros.

3.3 Procedimientos para el reporte y definición de fechas claves

Tras la definición de objetivos, alcance y metodología de reporte, el proceso de diseño continua con la definición más detallada de los procedimientos a utilizar dando respuesta a las siguientes interrogantes: ***¿Qué reportar y con qué frecuencia?***

La definición de los requisitos de la información para el reporte es vital para asegurar la calidad y consistencia de esta, en especial cuando hablamos de programas de gran envergadura que involucran el reporte de muchos usuarios. La información requerida puede variar a lo largo del tiempo de acuerdo a la experiencia ganada.

El contenido del reporte en términos generales debe incluir:

- Nombre, ubicación e información de contacto de la entidad que reporta.
- Nombre e información de contacto del representante designado por la entidad para el informe, firma y certificación del reporte.
- Periodo comprendido por el reporte y fecha de entrega
- Información de emisiones como el total de emisiones en toneladas métricas de CO_2, diferenciadas por emisiones directas e indirectas.
- Información de entrada utilizada en cálculos de emisión
- Metodología utilizada para la cuantificación de emisiones

- Declaración de auto-certificación y validación por terceros
- Información referente a metas de reducción de emisiones y medidas implementadas

Además se debe definir la frecuencia del reporte. La mayoría de los programas optan por una frecuencia anual (año calendario o año fiscal según jurisdicción). En cuanto al plazo del reporte es recomendable otorgar un margen de tiempo suficiente, de 2 a 4 meses, para que los agentes emisores preparen y verifiquen sus reportes. Por último, se debe establecer el periodo de tiempo de almacenaje de datos y registros. El tiempo definido está dado principalmente por la normativa legal vigente.

3.4 Plataformas para el reporte

El siguiente paso del proceso de implementación tiene por objetivo dar respuesta a las siguientes preguntas: ***¿Dónde reportar y quién tiene acceso a la información del reporte?***

La plataforma definida para el reporte y la administración de datos puede variar desde la forma más sencilla como una hoja de cálculo de un archivo Excel hasta un sofisticado sistema de reporte en línea. La definición de los atributos con que contará la plataforma estará dado por otras características del sistema como: Tipo de información, número de agentes emisores que reportarán, el tiempo requerido para el diseño y desarrollo del sistema de administración de datos, tipo de usuarios y que tan familiarizados se encuentran estos con el uso de sistemas en línea, costos de desarrollo y mantenimiento, disponibilidad de conocimiento técnico IT, requisitos de seguridad de la información, integración con otros sistemas, requisitos normativos vigentes, entre otros.

Al momento de diseñar un sistema para el reporte y manejo de datos, se deben tener en consideración los siguientes elementos:

Tabla 2. Elementos a considerar en el diseño de una plataforma para el reporte

Estructura estandarizada	El uso de formatos estandarizados para el reporte de emisiones mejora la consistencia y calidad de la información. También permite asegurar que la información suministrada sea la información requerida.
Incorporación de funciones para la disminución de errores	El diseño puede incluir funciones que ayuden a reducir el número de errores al momento del reporte en plataformas digitales, como por ejemplo: - *Restricción de los campos de datos de entrada* - *Definición de unidades de medidas, número y tipo de caracteres*

	- *Verificación automática de datos de entrada* - *Valores de factores de emisión pre-establecidos* - *Requisito de verificación de emisiones por más de un usuario* - *Notificación al usuario de errores en línea*
Incorporación de funciones para la verificación de emisiones	Implementación de herramientas que permitan la verificación de los datos reportados como la habilitación de permisos de acceso a organismos verificadores y terceros verificadores previo a la fecha de entrega del reporte (Declaración de verificación).
Seguridad y confidencialidad de la información	Asegurar la seguridad y confidencialidad de la información sensible para la organización o entidad que reporta mediante la implementación de herramientas como: - *Credenciales de ingreso a la plataforma* - *Actualización a intervalos regulares de tiempo de contraseñas* - *Doble autenticación (dos usuarios) de envíos y cambios de la información reportada* - *Establecimiento de ventanas de tiempo para el ingreso de datos* - *Diferenciación de usuarios y permisos según la función de cada usuario* - *Utilización de servidores seguros para el almacenamiento de datos*
Compatibilidad con otros sistemas de información	En el caso de sistemas integrados se debe asegurar que la información de ambos sistemas es compatible y no representa un riesgo de duplicidad de información. El sistema de reporte puede estar integrado además con sitios de interés como páginas web de normativas vigentes, manuales de ayuda, etc.
Validación documental virtual vs documentación en papel	Es de gran importancia establecer mediante la inclusión de una disposición en la reglamentación que tanto la documentación virtual como la documentación en papel tendrá el mismo peso y status para términos del reporte.

Una vez seleccionado el tipo de plataforma para el reporte de emisiones, se recomienda realizar pruebas piloto idealmente con usuarios reales, con la finalidad de identificar y posteriormente rectificar problemas técnicos, así como familiarizar al usuario con el sistema.

Por último pero no menos importante es la definición respecto del acceso a la información, específicamente que datos serán confidenciales y que datos podrán ser compartidos públicamente. La protección de la información, en especial aquella información comercialmente

sensible, es una preocupación mayor para quienes reportan, dado que esta puede ser utilizada por la competencia. Por esta razón resulta fundamental generar confianza dentro de los usuarios del sistema sin sacrificar la transparencia y el uso de la información reportada. Las medidas implementadas deben estar en concordancia con cualquier normativa legal asociada.

3.5 Medidas de control y aseguramiento de la calidad

La aplicación de medidas de control y aseguramiento de la calidad son fundamentales a la hora de asegurar la calidad y precisión de la información reportada. La elección de la medida más apropiada va a depender de los objetivos establecidos para el programa, el costo de las medidas y el número de usuarios que reportan, entre otros factores. Las medidas de control de calidad tienen su enfoque principalmente en las actividades involucradas en la preparación del reporte de emisiones: Cuantificación, monitoreo, validación de datos y reporte. Mientras que las medidas de aseguramiento de calidad se enfocan principalmente en la etapa de verificación.

En la siguiente tabla se presentan algunos ejemplos de medidas de aseguramiento y control de la calidad para diferentes etapas del ciclo de reporte:

Tabla 3. Medidas de control de calidad

Cuantificación y Monitoreo	**Implementación de un plan de monitoreo:** El Plan de monitoreo es considerado una de las herramientas más importantes para los agentes emisores, ya que compila la información más relevante del sistema de reporte, como por ejemplo: - *Información básica de la instalación incluyendo datos de contacto* - *Listado de las fuentes de emisión que deben ser monitoreadas* - *Datos de cálculo* - *Descripción del método de cuantificación* - *Responsables y plazos definidos para cada actividad* - *Evaluación de errores y fallos durante la recolección de información y monitoreo* - *Descripción de medidas de control para los errores y fallos detectados* Se recomienda la inspección en terreno del plan de monitoreo a fin de determinar el cumplimiento de los parámetros descritos en él.
Validación de datos	Incorporación de herramientas para la revisión en línea de la información reportada, como chequeo estadístico o algorítmico, etc. Ejemplos: Detección de campos sin información, valores fuera del rango esperado, comparación de información reportada versus datos del año

	anterior
Asistencia (Entrenamiento)	El entrenamiento del personal involucrado en las distintas etapas de un sistema de reporte es de vital importancia para asegurar el éxito del sistema de reporte. Especialmente en sistemas nuevos donde resulta necesario emplear recursos en la capacitación de los usuarios respecto de la metodología de reporte hasta alcanzar un potencial técnico acorde con los requerimientos del sistema. Cabe destacar, que el entrenamiento del personal involucrado debe extenderse no solo a una etapa inicial del sistema sino a lo largo de su ciclo de vida, dado los cambios en las metodologías de medición, normativas asociadas y la rotación de responsables asignados. Herramientas disponibles: - *Manuales, guías técnicas* - *Mesón de ayuda* - *Preguntas frecuentes* - *Cursos presenciales y en línea* - *Webinars, seminarios y conferencias*

Tabla 4. Medidas de Aseguramiento de calidad

Auto-Certificación	Corresponde a una auto-evaluación por parte del agente emisor respecto de las emisiones reportadas, donde certifica el cumplimiento de los requisitos del programa y la correcta estimación de las emisiones. El responsable de la auto-certificación es definido por la misma organización. Esta persona no debe tener participación en ninguna de las etapas del proceso de reporte. Al ser desarrollada por el mismo agente emisor, la auto-certificación se considera insuficiente en términos de confiabilidad, por lo cual es comúnmente complementada con otras medidas de verificación.
Revisión por encargados del programa	Como su nombre lo indica, corresponde a una revisión externa al agente emisor desarrollada por encargados del sistema. La revisión puede tener un enfoque documental o presencial. Y considera el desarrollo de actividades de auditoría y visitas en terreno. La estimación de los recursos necesarios para cubrir el desarrollo de estas actividades, resulta fundamental para asegurar el éxito de esta medida de aseguramiento a lo largo del tiempo.

Verificación por tercera parte	Verificación externa al agente emisor llevada a cabo por una tercera parte facultada para tales fines. Esta medida se ha definido como un requisito para la mayoría de los reportes de carácter obligatorio. En otros casos se utiliza como medida de verificación de reportes que presenten incongruencias o bajo niveles de confiabilidad de la información. La mayoría de los Sistemas de reportes definidos en la actualidad exigen que el organismo verificador base su proceso de verificación en estándares reconocidos como ISO 14.064-3 y cuenten con la acreditación otorgada por un organismo certificado para tales fines (Certificación ISO 17011). Sistemas que exigen la verificación por terceras partes deben establecer la frecuencia con que el organismo verificador debe ser cambiado a fin de evitar conflictos de intereses.

3.6 Medidas de coerción

Resulta necesario para el éxito de un Sistema de reporte la implementación de medidas de coerción que aseguren el reporte en conformidad y a tiempo por parte de los agentes emisores así como de los organismos verificadores. Las medidas deben estimular la participación y el cumplimiento de los objetivos establecidos. Y ante el caso de incumplimientos debe establecer las sanciones o medidas aplicables según el grado de estos. Las medidas de coerción pueden variar desde simples notificaciones hasta el inicio de acciones legales o multas en caso de violaciones graves a los requisitos del sistema.

4. APLICACIÓN AL CASO CHILENO

4.1 En relación al sistema MR definido para Chile

- **Respecto de la frecuencia de reporte**: Tanto la revisión de la experiencia internacional como las recomendaciones del Banco Mundial presentadas en este documento señalan que la frecuencia recomendada para el reporte de emisiones es anual. Aún más, el Banco Mundial sugiere un plazo entre 2 y 4 meses para la elaboración del reporte del período a reportar. Dado lo anterior se sugiere analizar la posibilidad de modificar la frecuencia trimestral de reporte actualmente vigente a una anual y exigir que el reporte de emisiones sea entregado junto con el informe de verificación en febrero del año siguiente al período a reportar.

- **Respecto de los establecimientos que deben reportar**: las recomendaciones del Banco Mundial indican una serie de posibles criterios para determinar qué establecimientos deben declarar sus emisiones: tipo de fuente, número de empleados, toneladas de producción, consumo de energía y límite de emisiones. La revisión de experiencia internacional arrojó que en su gran mayoría el criterio utilizado es el límite de emisiones (Quebec, British Columbia, California y México). En ninguno de los casos analizados el criterio era la potencia instalada. Importante mencionar que fue levantada insistentemente en las visitas a terreno la inquietud de que dado el criterio de potencia instalada habrían quedado fuera del listado establecimientos que emiten más que algunos que quedaron dentro dadas la horas de utilización de los equipos (a modo de ejemplo la industria pesquera señala que el % de utilización de sus calderas es bajo el 40% horas/año producto de los períodos de veda fijos). Dado lo anterior, se sugiere analizar para una futura ampliación/modificación de los impuestos verdes la posibilidad de: a) incorporar la tasa de utilización de los equipos en el criterio de selección, b) modificar el criterio de selección por alguno de los sugeridos por el banco mundial, o c) incluir establecimientos que dada su potencia instalada y % de utilización de sus fuentes se estime emiten más que el establecimiento que menos reportó el año 2017

- **Respecto a la Cuantificación y Monitoreo**: se sugiere estandarizar el contenido y nivel de detalle del Plan de Monitoreo que actualmente está contenido en la Metodología de medición presentada por el establecimiento y aprobada por la SMA.

4.2 En relación a la plataforma Impuesto Verde (SIV)

- **Respecto de la estandarización de la información**: Si bien el SIV estructura los reportes con el formato .csv, que es un estándar internacional de intercambio de datos vía archivos de texto, se considera necesario mencionar que el formato .csv no permite a los establecimientos realizar un doble chequeo, es decir, si el gerente de operaciones quisiera revisar los datos que un operador subió a la plataforma (qué es lo que en la práctica sucede de acuerdo al levantamiento realizado en las visitas a terreno) se encontraría con una serie de caracteres separados por coma de difícil lectura para revisar si la información es correcta. La recomendación es utilizar directamente .xls, como por ejemplo lo hace Suiza y la UE, ya que esto simplifica el proceso y disminuye errores de usuario.

- **Respecto de la incorporación de funciones para la disminución de errores:** se sugiere considerar a lo menos la posibilidad de implementar en el SIV la creación de perfiles distintos que permitan que un usuario ingrese los datos y sea otro el que después de revisarlos los envíe. Como ya se mencionó en el punto anterior, en las visitas a terreno se descubrió que en su gran mayoría no es el encargado de establecimiento quien ingresa los datos al sistema sino un tercera que varía según el establecimiento desde un mando medio, pasando por el encargado de calidad hasta un operador. El "doble chequeo" y procurar mediante la creación de un nuevo tipo de usuario que sea el encargado del establecimiento el que envíe los datos permitiría reducir errores.

- **Respecto de la seguridad y confidencialidad de la información:** Sugerimos evaluar la implementación de doble autenticación para envíos y cambios de información, y la diferenciación de perfiles por tipo de usuario (operacionales / gestores). La información debiese estar disponible al menos para el administrador general del sistema y el verificador.
  En términos de confidencialidad, en el sentido de quien tiene acceso a los datos, a nivel internacional el espectro es amplio, desde la experiencia del MDL donde los proyectos y sus datos son abiertos al público[1]; pasando por el Mecanismo de Compensación Suizo en el que el dueño del proyecto tiene la opción de dejar invisibles los datos que considere confidenciales; hasta el caso de Quebec que utiliza para el reporte de emisiones la misma plataforma de los impuestos que cuenta con un protocolo de seguridad de SSL que asegura la confidencialidad y la integridad de los documentos transmitidos entre las entidades y el gobierno.
  La Unión Europea exige a los sistemas automatizados que sean implementados por los países miembros como requisitos de funcionamiento: Proporcionar integridad de los datos, Confidencialidad a través del uso de técnicas de seguridad y encriptación,

[1] Ver http://cdm.unfccc.int/Projects/projsearch.html

Autentificación de datos (tanto el remitente como el receptor de los datos son conocidos y verificados) y No repudio de datos (técnicas de firma). Como requerimientos no funcionales exige: Control de acceso (Solo los miembros verificados pueden acceder), Disponibilidad (Asegurar la accesibilidad de los datos), Rastro de auditoria (Asegurarse que los cambios de datos puedan siempre encontrarse y analizarse en retrospectiva).

El sistema implementado por Alemania utiliza para la transmisión de datos entre el operador, el verificador y la autoridad, una Oficina Virtual de Envíos (VPS). Con el VPS, todas las partes involucradas pueden llevar a cabo comunicaciones digitales seguras y jurídicamente vinculantes, al proporcionar un estricto encriptado de extremo a extremo. Los usuarios necesitan descargar, instalar y configurar un cliente VPS en su computadora.

Desde un punto de vista técnico, la confidencialidad en VPS es provista por una clave pública criptográfica[2] (también conocida como criptografía asimétrica) como es el caso por ejemplo en el DEHST de Alemania. En este esquema de encriptación, dos claves relacionadas son utilizadas: una clave pública para encriptar el contenido y una clave privada para des encriptarlo. Esto asegura que solo el destinatario previsto (el que tiene la clave privada) pueda des encriptar y ver el contenido. La clave pública, como su nombre lo dice, es de acceso público y puede ser compartida. Para asegurar que la clave pública es válida y no proviene de un tercero malintencionado, puede ser almacenada en certificados digitales para ser transportada y compartida de manera segura. La manera más utilizada es una infraestructura de clave pública (PKI por sus siglas en inglés) donde entidades de certificación de confianza certifican la titularidad de claves. Otro beneficio de este esquema de encriptación es que permite asegurar la integridad de los datos dado que el proceso de des encriptación involucra una verificación de que el contenido original (encriptado) y el contenido resultante (des encriptado) coincidan. Cualquier cambio al contenido original produce una falla en el proceso de des encriptación.

- **Respecto a la validación de datos**: El SIV incorpora mecanismos de verificación en línea para campos sin información y algunos rangos de valores. Faltaría implementar algunos otros como por ejemplo: detección de formatos falsos (cuando se ingresan cifras en lugar de letras o al revés); comparación con la información reportada en periodos anteriores y otros chequeos cruzados como producción y balances de energía térmica en el caso del ETS de Suiza.

  Chequeos de plausibilidad permiten tener data de mejor calidad y disminuir las iteraciones con los establecimientos. Estos chequeos están un nivel más arriba que la validación de datos (orientada más bien a un valor en particular), al relacionar varios datos y permitir por ejemplo determinar si los datos recolectados están dentro de un rango y potencia razonable. Aún más, estos chequeos pueden ser utilizados para comparar datos de compañías y/o establecimientos similares.

2 https://en.wikipedia.org/wiki/Public-key_cryptography

- **Respecto de la asistencia y entrenamiento**: Es indispensable tener un canal confiable y expedito para recibir y dar respuesta oportuna a los establecimientos durante el período de reporte. Los plazos de respuesta deben ser conocidos y monitoreados, los usuarios deben poder hacer seguimiento a sus consultas y las preguntas frecuentes deben ser publicadas y actualizadas periódicamente.

5. RECOMENDACIONES PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN BASADAS EN LA ISO 27.001

A continuación se resumen los principales hallazgos del Diagnóstico de Ciberseguridad elaborado por Deloitte en las dependencias del Ministerio de Medio Ambiente (MMA) y la Superintendencia de Medio Ambiente (SMA) para la identificación de vulnerabilidades que ponen en riesgo la integridad de la información digital del sistema de medición, reporte y verificación diseñado para la aplicación del impuesto al carbono en Chile.

En total se identificaron 129 hallazgos, los cuales fueron clasificados en los 4 focos de acción que se presentan a continuación, ordenados de mayor a menor, según el número de hallazgos asociados a cada uno:

1. Vulnerabilidades lógicas: Revisión de seguridad lógica a los aplicativos VU, RETC y Termoeléctricas. Total hallazgos identificados: 59.

2. Gestión y Gobierno: Evaluación de la estructura de control interno de seguridad de la información. Total hallazgos identificados: 44.

3. Competencias: Evaluación de capacidades de profesionales y dotación de recursos humanos. Total hallazgos identificados: 17.

4. Vulnerabilidades físicas: Revisión de seguridad física a los centros de datos. Total hallazgos identificados: 9.

Los hallazgos fueron evaluados como alto, medio, bajo u oportunidad de mejora (OM) en base a su criticidad. Para efectos prácticos de este resumen, el reporte se enfocará en los hallazgos de criticidad alta. Para cada uno de ellos se hará mención de su potencial impacto y se entregarán recomendaciones para la mejora.

5.1 Vulnerabilidades lógicas

Para la detección de vulnerabilidades lógicas se verificaron las disposiciones de seguridad para un conjunto de activos TIC y la ejecución de ethical hacking a los aplicativos Ventanilla única (VU), RETC y Sistema Termoeléctrica.

Tabla 5. Resumen de hallazgos criticidad alta

Hallazgo	*Descripción*	*Recomendación*
Funcionalidad insegura para la subida de archivos	Aplicaciones cuentan con funcionalidades que permiten la subida de archivos, en algunos casos anónimamente. Además se evidenció la ausencia de medidas de seguridad que verifiquen el tipo y contenido del archivo subido. Un usuario malintencionado podría aprovechar estas vulnerabilidades para la subida de archivos con malware.	a.- Considerar todo contenido susceptible de ser modificado por el usuario como contenido no seguro. b.- Todos los archivos subidos deben ser examinados.
Detección de vulnerabilidad "Directory Transversal"	Se pueden obtener archivos que forman parte del sistema de archivos del servidor de manera anónima. Un usuario malintencionado podría aprovechar estas vulnerabilidades para la descarga anónima de archivos.	Implementación de mecanismos de validación de datos de entrada (tipo de dato esperado, longitud y caracteres permitidos).
Cross site scripting (XSS) persistente	Esta vulnerabilidad permite que un usuario malicioso ingrese un código JavaScript, el cual es almacenado por la aplicación. Posteriormente, este código podría ser ejecutado por un usuario tras acceder al navegador web. Lo anterior podría ser utilizado para la obtención de información sensible de la víctima.	a.- Implementar la validación de parámetros de entrada recibidos de los usuarios, a modo de evitar caracteres especiales y/o códigos inyectados. b.- Implementación de firewall para bloquear posible contenido malicioso incluido en peticiones HTTP.
Software desactualizado	Termoeléctricas: OpenSSL, Microsoft IIS VU: PHP El uso de software desactualizado representa un riesgo dado que las vulnerabilidades de estos softwares son de conocimiento público.	Actualización de servicios afectados o aplicación de parches se seguridad disponibles.
Biblioteca de terceros desactualizadas o no soportadas	VU: PHP Mailer RETC: PHP Easy Download VU: reCAPTCHA PHP (no soportada) El uso de bibliotecas de terceros desactualizadas representa un riesgo dado que las vulnerabilidades de estas son de conocimiento público.	Actualización de servicios afectados a la última versión disponible o la sustitución por otras bibliotecas conocidas y mantenidas que sirvan para el mismo propósito.
Cross Site Request Forgery (CSRF)	No se cuenta con mecanismos contra ataques de cross-site request forgery. Es decir usuarios podrían acceder a sitios afectados y hacer	Implementar patrón "Synchronizer Token Pattern" asociado a la cual sesión del usuario.

	click a URL modificados que habilitarían la sesión del usuario para uso malicioso.	
Debilidades en la funcionalidad para filtrar consultas SQL	Filtro de caracteres maliciosos deficiente para consultas de SQL. Esto podrías ser utilizado para la inyección de SQL malicioso.	Implementar metodología de consulta a través de "prepared statements" en lugar de concatenación de strings.
Tokens (IDs) predecibles	Usuario malicioso podría utilizar herramientas automatizadas que permitan la obtención de pre-imágenes de estos tokens para la creación de tokens propios que faculten la descarga automática de documentos subidos por usuarios de forma anónima.	a.- Utilización de funciones hash a colisiones, cuyo espacio de salida no permita emplear ataques de fuerza bruta. b.- No utilizar numeración secuencial
Software no soportado por fabricante	El software no soportado por el fabricante podría tener vulnerabilidades que son de dominio público, representando un riesgo para la integralidad, confidencialidad y disponibilidad de la información alojada en los recursos afectados.	Actualización de servicio afectado a la última versión disponible y soportada por el fabricante. Aquellos sistemas que no puedan migrarse debieran ser respaldados con medidas de control adicionales.
Inclusión remota de archivos	Se detectó que la aplicación permite la descarga de archivos "png" obtenidos de recursos remotos, mediante la manipulación de parámetros. Esto podría ser para la carga de códigos maliciosos dentro de archivos "png".	Implementar sistema de sanitización y validación de datos de entrada recibidos.
Proceso de parches y actualización de seguridad incompleto	No se han instalado todos los parches de seguridad y actualizaciones de las siguientes plataformas: MMA: Servidor de dominio, servidor de respaldos SMA: Servidor antivirus, servidor archivos Higuera, Servidor Web server	a.- Instalación de parches de seguridad faltantes b.- Realización de pruebas a sistemas cuando se instalen los nuevos parches.

Tabla 6. Resumen de otros hallazgos

Hallazgo	**Criticidad**		
	Media	**Baja**	**OM**
Archivos sensibles accesibles anónimamente	**X**		
Comunicación no cifrada	**X**		
Datos sensibles enviados en texto plano	**X**		
Software no soportado por fabricante	**X**		
Contraseñas sin enmascarar	**X**		
Enumeración de usuarios	**X**		
Inadecuada política de contraseña	**X**		
Debilidades en el almacén de contraseñas en la base de datos	**X**		
Robo de sesión posible	**X**		

Validación de permisos de acceso inadecuada	**X**		
Configuración de protocolo SSL/TLS débil	**X**		
Cookie no protegida por atributo HttpOnly	**X**		
Posibilidad de ataques de denegación de servicio a través de consultas SQL	**X**		
Claves de acceso o Password poco robustas	**X**		
Cuentas usuario en servidores de dominio deben ser verificadas	**X**		
Certificado SSL/TLS no confiable		**X**	
Contraseña no requerida para modificar información de usuario		**X**	
Session Fixation		**X**	
Manejo de errores inadecuado		**X**	
Cookie no protegida por el atributo secure		**X**	
Archivos de prueba y desarrollo publicados en producción		**X**	
Bloqueo de cuentas inexistente		**X**	
Autenticación múltiple permitida		**X**	
Múltiples métodos HTTP habilitados		**X**	
Funcionalidad de cambio de contraseña no disponible		**X**	
Identificación de dirección IP interna		**X**	
Información interna en documentos públicos		**X**	
Listado de directorio habilitado		**X**	
Páginas habilitadas por defecto		**X**	
Inexistencia de protección contra IFRAMES		**X**	
Autocomplete no declarado		**X**	
Métodos HTTP extendidos habilitados		**X**	
Acceso a archivo de Log anónimamente		**X**	
Inadecuada configuración de encabezados de seguridad		**X**	

5.2 Gestión y Gobierno

Para el diagnóstico del nivel de Gestión y Gobierno de Seguridad de la Información se realizaron entrevistas con colaboradores de MMA y SMA donde se evaluó la Política, procedimientos y la práctica de aspectos de seguridad TIC en base al estándar internacional ISO 27002 "Código de práctica para controles de seguridad de la información" y los 35 objetivos de control del estándar ISO/IEC 27001.

Tabla 7. Resumen de hallazgos criticidad alta

Hallazgo	*Lugar*		*Descripción*	*Recomendaciones*
	MMA	*SMA*		
Documentación de Desarrollo de sistemas y seguridad no identificada	**X**		No se observó la existencia de una política de desarrollo y mantención de sistemas que contemple aspectos de seguridad de la	Formalizar la documentación citada, así como protocolos para la encriptación de autenticaciones y

			información, así como procedimientos formales de prueba, calidad de los sistemas y el paso a producción. Esto podría generar incidencias que afecten la confidencialidad, integridad y disponibilidad de aplicaciones realizadas por MMA o algún proveedor.	transferencia de datos sensibles en aplicaciones web. También desarrollo seguro de aplicaciones web.
Carencia de conceptos y disposiciones de ciberseguridad en Política de Seguridad de la Información	**X**		Se observó que Política de Seguridad de la información no incluye definiciones, normas, conceptos y disposiciones de ciberseguridad. La ausencia de lo anterior repercute en la correcta implementación de controles que aseguren la confidencialidad, disponibilidad e integridad de los datos.	Incorporar a Política de Seguridad de la Información conceptos de ciberseguridad y/o adherir a un estándar internacional como ISO 27032.
Aspectos de Gestión de Cambios no documentados	**X**	**X**	Si bien se evidenció la existencia de prácticas de gestión de cambios estas no se encuentran documentadas. Tampoco existe un comité que evalúe las solicitudes y lleve el control de los registros asociados. La ausencia de lo anterior permite la falta parcial o completa de controles, previo la producción de un nuevo sistema o funcionalidad.	Implementar: a.- Procedimiento formal y registros asociados b.- Ajustar alcance a sistemas, infraestructura y usuarios c.- Definir responsable o comité para la evaluación y aprobación de solicitudes, así como el monitoreo de los avances.
Segregación de funciones no aplicada a Encargado de Seguridad	**X**	**X**	El responsable de Seguridad de la información, es la misma persona que lidera operaciones tecnológicas e infraestructura TIC. La dualidad de funciones compromete la independencia operativa dada la contraposición de ambos cargos en cuanto a objetivos y alcance.	Separación de funciones.
Ausencia de prácticas y documentación de continuidad de negocio (BCP)	**X**	**X**	La ausencia de procedimientos y documentos sobre un plan de continuidad de negocios pone en riesgo la operación y su recuperación en caso de contingencia.	Creación de un plan de continuidad del negocio (BCP) y un plan de recuperación ante desastres tecnológicos (DRP) que defina estrategias, recursos y procedimientos.

Tabla 8. Resumen de otros hallazgos

Hallazgo	*Lugar*		Criticidad		
	MMA	*SMA*	Media	Baja	OM
No se evidencian sesiones de Comité de Seguridad de la Información	X		X		
Falta de empoderamiento de Rol Encargado de Seguridad de la Información	X		X		
Actividades de alta, baja y modificación no formalizadas o difundidas	X		X		
Gestión de acceso no formalizada en procedimiento	X		X		
Procedimientos y Política de Seguridad de la Información no relacionados	X				X
Capacitación y Difusión deficiente respecto a Seguridad de la Información	X	X	X		
Aspectos de criptografía no aplicada	X	X	X		
Política de Seguridad de la Información no contempla aspectos de capacitación y difusión	X	X	X		
Carencia de una línea Base de Seguridad Formal	X	X	X		
Gestión de Incidentes incompleta	X	X	X		
Gestión de LOGS sin formalizar ni comunicar	X	X	X		
Procedimientos de Parches y Releases no documentados formalmente	X	X	X		
Programa anual de Auditoria no contempla aspectos de seguridad de la información en todas sus revisiones	X	X	X		
Modelo de datos no se relacionan entre sí para la integración de sistemas con otras instituciones	X	X	X		
Ausencia de procedimiento que identifique, monitoree y regule las disposiciones legales	X	X	X		
Procedimiento ABM sin aprobación		X		X	
Metodología de desarrollo de sistemas no actualizada		X		X	
Estructura de roles y perfiles no compartidos	X	X		X	
Bajo nivel de contacto con grupos de interés	X	X		X	
Políticas y procedimientos de escritorio limpio no forman parte de un plan. No son controlados	X	X		X	
Procedimientos de monitoreo sin documentar ni formalizar	X	X		X	

5.3 Competencias

Para la detección de vulnerabilidades de competencias se realizó una visita a las instalaciones de MMA y SMA que contempló revisión de documentación y entrevistas al personal. El estándar internacional ISO 27003 (Anexo B) fue utilizado como marco de referencia.

Tabla 9. Resumen de hallazgos criticidad alta

Hallazgo	*Lugar*		*Descripción*	*Recomendaciones*
	MMA	*SMA*		
Duplicidad de roles – Encargado de Seguridad de la información	**X**	**X**	El responsable de Seguridad de la información, es la misma persona que lidera operaciones tecnológicas e infraestructura TIC. La dualidad de funciones compromete la independencia operativa dada la contraposición de ambos cargos en cuanto a objetivos y alcance.	Separación de funciones.
Vacantes no cubiertas	**X**	**X**	**Especialista de Redes y Monitoreo de seguridad de Redes (MMA)** **Prevencionista de Riesgos (MMA-SMA)** Actividades relacionadas con redes no cubiertas, lo que representa un riesgo ante el caso de ataque a redes.	Cubrir vacantes ausentes o en su defecto actividades no cubiertas.
Indisponibilidad de personal VU y RETC – Gestión de Incidentes Mesa de Ayuda	**X**		La gestión de incidentes de la mesa de ayuda (VU y RETC) es realizada por alumnos en práctica, los cuales son renovados cada 3 meses, resultando en una atención de incidentes ineficiente y poco estable.	Dar continuidad al servicio de mesa de ayuda.
Ausencia de Rol	**X**	**X**	Cargo: Gestión de cambios independiente y transversal a la institución. Especialista Operativo de Seguridad de la información. La falta de asignación de un responsable podría dar paso a producción de piezas de software defectuosas, vulnerables no autorizadas en el caso del rol de Gestión de cambios.	Implementar rol.
Ausencia de Auditoria de Seguridad de la Información periódica	**X**		El departamento a cargo de auditorías no considera dentro de su alcance la ejecución de	Incluir dentro del programa anual de auditorías las áreas tecnológicas.

			auditorías tecnológicas o relacionadas con la seguridad de la información. Esto repercute en la falta de control interno en aspectos de seguridad de la información.	
Baja periodicidad de auditoria de seguridad de la información		**X**	Periodicidad podría ser insuficiente para asegurar el cumplimiento de los controles mínimos de seguridad.	Incluir dentro del programa anual de auditorías las áreas tecnológicas.
Actividades no cubiertas respecto a monitoreo de seguridad de redes activo		**X**	La práctica del rol de monitoreo de seguridad de redes no ha sido documentado, aprobado ni comunicado. Este hecho podría representar un riesgo en caso de algún ataque a las redes.	Documentar actividades.

Tabla 10. Resumen de otros hallazgos

Hallazgo	***Lugar***		**Criticidad**		
	MMA	***SMA***	**Media**	**Baja**	**OM**
Inexistencia de periodicidad y condiciones mínimas para sesionar comité de seguridad	**X**		**X**		
Ausencia de Administración de riesgos orientados a la seguridad de la información	**X**	**X**	**X**		
Tratamiento de incidentes de seguridad no adhiere a estándares de calidad		**X**	**X**		

5.4 Vulnerabilidades físicas

Para la detección de vulnerabilidades físicas se realizó una visita en terreno de los centros de datos y sistemas de apoyo utilizados en MMA y SMA. Las condiciones de estos fueron evaluadas de acuerdo al estándar internacional NIST 800-53.

Tabla 11. Resumen de hallazgos criticidad alta

Hallazgo	*Lugar*		*Descripción*	*Recomendaciones*
	MMA	*SMA*		
Sitio Alternativo Inexistente	**X**	**X**	Instituciones no cuentan con sitio alternativo en caso de contingencia (incendio, terremoto) lo cual pone en riesgo la continuidad del negocio.	Implementación de sitio alternativo. Asignación de VPN para trabajo de forma remota.
Brecha de Seguridad en Acceso físico	**X**		Existe brecha de seguridad que involucra a grupo electrógeno. Posible riesgo de acceso no autorizado e interrupción total o parcial de servicio de energía.	Mejorar seguridad del área. Implementación de cámaras de seguridad.
No existe segregación física de áreas técnicas		**X**	Datacenter se encuentra colindante a otras áreas no pertenecientes a tecnología lo que permite el acceso a zonas sensibles de personal no autorizado.	Habilitar espacio físico sólo para personal TIC.
Aire acondicionado de precisión inexistente		**X**	Aire acondicionado no es de precisión. Efectos potenciales: Desgaste acelerado de sistema de aire por sobre exigencia, Indisponibilidad de servicios TIC	Implementar equipos de precisión.
Falta de contratos de Mantenimiento	**X**	**X**	Equipos de energía, aire acondicionado, ups y sistema de extinción de incendios no cuentan con contratos de mantención preventiva.	Implementar mantenimiento preventivo de equipos señalados.

Tabla 12. Resumen de otros hallazgos

Hallazgo	*Lugar*		Criticidad		
	MMA	*SMA*	Media	Baja	OM
Procedimientos no formalizados (De actividades operacionales, monitoreo y seguridad)	**X**	**X**	**X**		