INFORME Nro. DFOE-GOB-IF-00016-2022

9 de diciembre, 2022

INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE INFORMACIÓN EMPRESARIAL COSTARRICENSE (SIEC) EN EL MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMERCIO

2022

Contraloría General de la República, Costa Rica
División de Fiscalización Operativa y Evaluativa
Área de Fiscalización para el Desarrollo de la Gobernanza
P3-01-GE-01 V6

CONTENIDO

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Resumen Ejecutivo

¿Qué examinamos?

La presente auditoría tuvo como objetivo determinar si la gestión de la seguridad de la información del Sistema de Información Empresarial Costarricense, en adelante SIEC, cumple razonablemente con lo establecido en el marco jurídico y técnico aplicable. Para ello se valoró específicamente el Gobierno y Gestión de las Tecnologías de Información y el Sistema de Gestión de la Seguridad de la Información, en el período comprendido entre el 01 de enero 2020 y el 30 de junio 2022.

¿Por qué es importante?

El Ministerio de Economía, Industria y Comercio (MEIC) apoya el desarrollo económico y social del país a través de políticas que facilitan un adecuado funcionamiento del mercado, la protección de los consumidores, la mejora regulatoria, el fomento de la competitividad y el impulso de la actividad empresarial, especialmente para las micro, pequeñas y medianas empresas (PYME), facilitando los encadenamientos productivos, mejorando la capacidad estatal de administrar el comercio, velando por la competencia justa, la mejora regulatoria, la calidad y el apoyo al consumidor. Como parte de los instrumentos para el desarrollo de dichas competencias cuenta con el SIEC, un sistema crítico que soporta la labor que desempeña la Dirección General de la Pequeña y Mediana Empresa (DIGEPYME), para el fortalecimiento competitivo y sostenible de las PYME costarricenses. En ese contexto, resulta necesario garantizar la seguridad de la información contenida en dicho sistema, cuyo funcionamiento responde además al mandato de su ley de creación, y por lo tanto, requiere ser protegido de ataques, daños, accesos no autorizados o cualquier otra amenaza.

¿Qué encontramos?

Se identificaron debilidades que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información contenida en los sistemas sustantivos del MEIC, lo que incluye entre otros al SIEC, resultando que dicho sistema no necesariamente satisface las necesidades del negocio ya que presenta oportunidades de mejora en materia de funcionalidad y seguridad. Lo anterior podría incidir en la capacidad operativa del Departamento de Tecnologías de Información (DTI) y generar afectación a los usuarios, pues la calidad, oportunidad y continuidad de la prestación de los servicios que brinda el MEIC está directamente relacionada con los procesos ejecutados por TI para soportar los sistemas.

En lo que respecta al eje de ***Gobierno y Gestión de las Tecnologías de Información,*** *se determinó que falta definir y aprobar un "Marco de gobierno y gestión de tecnologías de información"; y que existen debilidades en los procesos establecidos e implementados por el MEIC para gestionar las tecnologías de información, particularmente en: gestión de servicios de TI (mesa de ayuda), gestión de incidentes y problemas, gestión de cambios, mantenimiento preventivo y correctivo y gestión de versiones y configuraciones. La falta de definición en esta materia incide en la toma de decisiones y en las capacidades y cobertura que presenta el área técnica; afecta a todos los procesos de TI del MEIC y por ende los principios básicos de seguridad; y pone en riesgo el cumplimiento de los objetivos estratégicos tanto de TI como del negocio.*

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Además, se determinó que el MEIC en lo que respecta a ***la Gestión de la Seguridad de la Información****, no ha definido un sistema de gestión de seguridad de la información (SGSI) con sus diferentes componentes, y presenta debilidades en aspectos tales como el marco de gestión de seguridad de información, sensibilización en seguridad de información, políticas relativas a seguridad de información, seguridad lógica, continuidad de negocio, respaldo y recuperación. La falta de orientación en materia de seguridad de información, alineada con los objetivos institucionales, puede tener efectos adversos sobre la confidencialidad, la disponibilidad y la integridad de la información, es decir, se compromete todo esfuerzo de la administración para proteger sus activos dado que no se conocen los escenarios de riesgos a los que se enfrenta el equipo de TI y la organización como un todo; y suele asociarse con la posibilidad de dejar abiertos portillos que pueden ser explotados por un atacante; por ejemplo, el uso de usuarios genéricos no controlados podría facilitar la escalación de privilegios en la red o el acceso no autorizado si se combina con otras vulnerabilidades en el entorno web.*

¿QUÉ SIGUE?

Se emiten disposiciones al Ministro de Economía Industria y Comercio con el propósito de impulsar la implementación gradual de un marco de gobierno y gestión de TI y el marco de seguridad de información que utilizará el MEIC en adelante, para lograr la implementación del Sistema de Gestión de Seguridad de la Información. De igual forma, se le solicita tomar acciones para gestionar lo correspondiente en cuanto a la Política de Continuidad de Negocio y Análisis de Impacto de Negocio (BIA). *Las definiciones técnicas y la integración de actividades quedarán en manos del Comité Gerencial de TI.*

.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

DIVISIÓN DE FISCALIZACIÓN OPERATIVA Y EVALUATIVA
ÁREA DE FISCALIZACIÓN PARA EL DESARROLLO DE LA GOBERNANZA

INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE INFORMACIÓN EMPRESARIAL COSTARRICENSE (SIEC) EN EL MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMERCIO

1. Introducción

ORIGEN DE LA AUDITORÍA

1.1. El estudio se efectuó con fundamento en las competencias que le confieren a la Contraloría General de la República (CGR) los artículos 183 y 184 de la Constitución Política, 12 y 21 de su Ley Orgánica, Nº. 7428.

1.2. La auditoría se realizó en cumplimiento del Plan Anual Operativo de la División de Fiscalización Operativa y Evaluativa y sus modificaciones, con fundamento en las competencias que le son conferidas a la Contraloría General de la República en los artículos 183 y 184 de la Constitución Política y los artículos 12, 17 y 21 de su Ley Orgánica, N° 7428.

1.3. Al Ministerio de Economía, Industria y Comercio (MEIC) le corresponde apoyar el desarrollo económico y social del país a través de una participación en políticas que faciliten un adecuado funcionamiento del mercado, la protección de los consumidores, la mejora regulatoria, el fomento de la competitividad y el impulso de la actividad empresarial. Fue creado mediante la Ley Nº 2656 del 4 de noviembre de 1960, la cual fue reformada y se tiene hoy vigente como Ley Orgánica la N° 6054 del 14 de junio de 1977, teniéndose además regulado en relación a su estructuración actual y vía Reglamento, el Decreto Ejecutivo N° 37457-MEIC del 2 de noviembre de 2012.

1.4. Desde su misión se marca que la institución "propicia y apoya el desarrollo económico y social por medio de políticas que faciliten el fortalecimiento de la competitividad de los sectores industria, comercio y servicios, especialmente las micro, pequeñas y medianas empresas (PYME), fomentando los encadenamientos productivos, mejorando la capacidad estatal de administrar el comercio, velando por la competencia justa, la mejora regulatoria, la calidad y el apoyo al consumidor". Esto se refleja en los objetivos estratégicos dentro de los cuales se destaca:

Fortalecer y consolidar los emprendimientos, la micro, pequeña y mediana empresa;

Facilitar condiciones que permitan el acceso y el adecuado funcionamiento del mercado nacional, que favorezcan el desarrollo integral y equitativo del país.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

1.5. Como mecanismo de soporte al proceso de registro y certificación de PYMES se implementa el Sistema de Información Empresarial Costarricense (SIEC) para registrar PYMES, producción, exoneraciones, emitir constancias, entre otros. Este sistema permite procesar información de naturaleza económica vinculada a personas naturales, por lo que es relevante asegurar que la plataforma que soporta el sistema cumpla con los principios de confidencialidad, disponibilidad e integridad para favorecer la salvaguarda de los activos de TI que incluye tecnología, procesos, información y personal.

Objetivo

1.6. Determinar si la gestión de la seguridad de la información del SIEC cumple razonablemente con lo establecido en el marco jurídico y técnico aplicable.

Alcance

1.7. El estudio abarcó la gestión de la seguridad de la información del SIEC. Comprende el periodo entre el 1 de enero 2020 y el 30 de junio 2022.

Criterios de Auditoría

1.8. Los criterios de auditoría se comunicaron mediante oficio N.º 11902 (DFOE-GOB-0303), del 15 de julio del 2022, y se expusieron al Sr Luis Guillermo Rojas, Jefe del Departamento de TI y al Sr Roberto Alvarado, Director de DIGEPYME en una sesión virtual utilizando la herramienta de Google Meet y celebrada el 11 de julio de 2022.

Metodología aplicada

1.9. La auditoría se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público, con el Manual General de Fiscalización Integral de la CGR y el Procedimiento de Auditoría vigente, establecido por la DFOE.

1.10. Para la elaboración de esta auditoría se utilizaron las técnicas y procedimientos estipulados en el Manual General de Fiscalización Integral (MAGEFI) de la Contraloría General de la República. Además, se observó en lo atinente, las disposiciones contenidas en las Normas Generales de Auditoría para el Sector Público (NGASP), y demás normativa aplicable.

1.11. Además, se utilizó la información suministrada en las entrevistas a funcionarios del Ministerio de Economía industria y Comercio, así como las respuestas a las consultas planteadas por escrito ante el Departamento de TIC, la Auditoría Interna y las unidades de negocio relacionadas con el sistema.

1.12. También, se realizaron pruebas sustantivas para validar la efectividad operativa de controles específicos tanto a nivel de aplicación como a nivel de gestión de TI. Además se realizaron pruebas a la plataforma web en busca de vulnerabilidades conocidas y el resultado se reportó a la administración con carácter de confidencialidad.

Aspectos positivos que favorecieron la ejecución de la Auditoría

1.13. Como parte de los aspectos positivos a resaltar, se encuentra la colaboración prestada por parte de la Administración y en particular su equipo de TI, además del apoyo de la Auditoría Interna del MEIC.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Limitaciones que afectaron la ejecución de la Auditoría

1.14. No se presentaron situaciones que limitaron el desarrollo normal del estudio, si bien se tuvo dificultades para obtener algunos datos de forma que fueran comparables, fue posible recopilar información suficiente para obtener conclusiones.

Generalidades acerca de la seguridad de la información del SIEC en el MEIC

1.15. La seguridad de la información comprende un conjunto de medidas preventivas y reactivas de las organizaciones con el fin de resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

1.16. El estudio considera las tres variables clave de la seguridad, a saber: confidencialidad, disponibilidad e integridad, las cuales se analizaron en el contexto de los controles implementados por la administración para asegurar la salvaguarda de los activos de información. Además se evalúan los procesos de TI que soportan la seguridad. Seguidamente, se detallan las oportunidades de mejora más relevantes que se identifican como resultado del examen de los principales controles relacionados con la seguridad de la información.

1.17. La DIGEPYME es la dirección responsable por el proceso de registro y certificación de PYMES y en atención a su cometido se implementó en 2008 el Sistema de Información Empresarial Costarricense, como una solución que permite captar información de personas y de empresas. Este sistema requiere una actualización o la creación de una versión nueva que facilite la consulta y la interconexión con otras entidades.

1.18. Como sistema, el SIEC hace parte de un inventario de recursos de TI, y de una infraestructura que es gestionada y soportada por la Dirección de TI. En consecuencia las acciones que realiza TI en materia de gestión, inciden directamente sobre la prestaciones de seguridad del sistema, las actividades operativas de TI como mantenimiento, actualización, configuración, respaldos, etc hacen parte de los controles generales de TI que respaldan el cumplimiento en materia de seguridad.

1.19. La gestión de la seguridad es un fenómeno más que técnico, organizacional, que le compete a todos los niveles de mando, la definición de la estrategia de seguridad y la programación de proyectos para implementar controles es una labor de gobierno que debe ser emprendida por la alta gerencia en coordinación con el departamento de TI, por ende evaluar la calidad de la toma de decisiones en materia de seguridad es importante para alcanzar una postura de seguridad aceptable.

Comunicación preliminar de los resultados de la Auditoría

1.20. Los resultados de la auditoría se presentaron verbalmente el día 29 de noviembre de 2022 por medio de la plataforma Google Meet administrada por CGR, con la participación de los señores: Ayleen Marín, representante del Despacho; Luis Araya Carranza, Auditor Interno; Marlene Morera, Especialista Auditoría Interna; Roberto Alvarado, Director DIGEPYME; Jose Arce, Jefe de Registro de DIGEPYME; Denis Gaitán, Especialista en TI; Karol Cristina Chacón, representante de Asesoría Jurídica y Luis Guillermo Rojas, Director de TI. Al respecto, se recibieron observaciones en la sesión de presentación por parte de la administración, las cuales fueron atendidas y consideradas en el documento final.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

SIGLAS

1.21. La descripción de las siglas utilizadas en este documento se detalla a continuación:

Sigla	**Significado**
CGR	Contraloría General de la República
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
LGCI	Ley General de Control Interno
NGASP	Normas Generales de Auditoría para el Sector Público
MAGEFI	Manual General de Fiscalización Integral
TIC	Tecnología de Información y Comunicaciones
ISO	Organización Internacional para la Estandarización, por sus siglas en inglés
COBIT	Objetivos de Control para Información y Tecnologías Relacionadas, por sus siglas en inglés
RPO	Objetivo de Punto de Recuperación, por sus siglas en inglés
RTO	Objetivo de Tiempo de Recuperación, por sus siglas en inglés
BIA	Análisis de Impacto de Negocio, por sus siglas en inglés
BCP	Plan de Continuidad de Negocio, por sus siglas en inglés
DRP	Plan de Recuperación en caso de Desastre, por sus siglas en inglés

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2. Resultados

Gobierno y Gestión de Tecnología de Información

2.1. La capa en la que se opera o se implementa el gobierno de TI es la gestión, un espacio en el que los mandos medios dirigen la organización para alcanzar objetivos trazados por el nivel directivo, como función implica administrar todos los recursos disponibles (técnicos, de procesos, humanos, físicos, presupuestarios, culturales, conocimiento, etc.), y armonizar las actividades desplegadas, de forma tal que aporten valor a la institución, minimicen el riesgo y optimicen el uso de recursos.

Ausencia de un "Marco de gobierno y gestión de tecnologías de información" en el MEIC

2.2. La Ley General de Control Interno, Ley 8292 en su artículo 16 señala la responsabilidad del jerarca y los titulares subordinados en cuanto a los sistemas de información, e indica que este deberá entre otras cosas: "Contar con procesos que permitan identificar y registrar información confiable, relevante, pertinente y oportuna; asimismo, que la información sea comunicada a la administración activa que la necesite, en la forma y dentro del plazo requeridos para el cumplimiento", así como "armonizar los sistemas de información con los objetivos institucionales y verificar que sean adecuados para el cuido y manejo eficientes de los recursos públicos".

2.3. La derogación de las normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CO-DFOE), resolución R-CO-26-2007, y modificación de las normas de control interno para el sector público, resolución de la Contraloría General de la República, R-DC-17-2020, en el transitorio I dispuso que "Todas las instituciones, entidades, órganos u otros sujetos pasivos de la fiscalización de la Contraloría General de la República deberán haber declarado, aprobado y divulgado el marco de gestión de las tecnologías de información y comunicación, requerido en la modificación incorporada en esta resolución a las Normas de Control Interno para el Sector Público (N-2-2009-CODFOE), a más tardar el 1° de enero del 2022".

2.4. Las Normas de Control Interno para el Sector Público (N-2-2009CO-DFOE), en el ítem 5.9 señala que de conformidad con el perfil tecnológico de la institución, órgano o ente, en función de su naturaleza, complejidad, tamaño, modelo de negocio, volumen de operaciones, criticidad de sus procesos, riesgos y su dependencia tecnológica, el jerarca deberá aprobar el marco de gestión de tecnologías de información y establecer un proceso de implementación gradual de cada uno de sus componentes.

2.5. Por otra parte, Cobit 5, en su capítulo 4, relacionado con "El Modelo de Referencia de Procesos COBIT 5", establece en cuanto a los procesos de Gobierno y Gestión que "Una de las directivas en COBIT es la distinción hecha entre gobierno y gestión. En línea con este principio, se espera que todas las empresas implementen varios procesos de gobierno y varios procesos de gestión para proporcionar un gobierno y una gestión del entorno IT exhaustivos.". Al considerar los procesos para gobierno y gestión, la diferencia entre los tipos de procesos se encuentra en los objetivos: Los procesos de gobierno tratan de los

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

objetivos de gobierno de las partes interesadas, entrega de valor, optimización del riesgo y de recursos, e incluye prácticas y actividades orientadas a evaluar opciones estratégicas, proporcionando la dirección de TI y supervisando la salida (Evaluar, orientar y supervisar); por su parte, los procesos de gestión cubren las áreas de responsabilidad de TI de la empresa y tienen que proporcionar cobertura de TI extremo a extremo en lo que atañe a soporte, mantenimiento y operación de sistemas.

2.6. Asimismo, Cobit 5 señala en su proceso APO01 sobre gestión del marco de TI que se deberá "Definir la estructura organizativa (APO01.01), Establecer roles y responsabilidades (APO01.02), Mantener los elementos catalizadores del sistema de gestión (APO01.03), Comunicar los objetivos y la dirección de gestión (APO01.04) (…)".

2.7. Cobit 5 en su práctica de gestión APO01.01 Establecer Roles y Responsabilidad señala la necesidad de establecer una estructura organizativa interna y externa que refleje las necesidades del negocio y las prioridades de TI. Implementar las estructuras de gestión requeridas (p. ej., comités) para permitir que la toma de decisiones se lleve a cabo de la forma más eficaz y eficiente posible".

2.8. Lo anterior se complementa con las prácticas señaladas en el proceso APO02 sobre gestión de estrategia, que busca "Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado". Este proceso contempla actividades de detalle como las siguientes "Evaluar el entorno, capacidades y rendimiento actuales (APO02.02), Definir el objetivo de las capacidades de TI (APO02.03), (...) Definir el plan estratégico y la hoja de ruta (APO02.05) y Comunicar la estrategia y la dirección de TI" (APO02.06).

2.9. En el particular del proceso de gestión de cambios el proceso BAI06 de Cobit 5, establece la necesidad de gestionar todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura.

2.10. En relación con la Gestión de incidentes y problemas COBIT 5 en el proceso DSS02, define la necesidad de proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes; lo cual implica recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.

2.11. La norma ISO IEC 27001:2014, Técnicas de seguridad - Sistemas de gestión de la seguridad de la información, es una buena guía para gestionar la mesa de ayuda y los incidentes que se reportan por esa vía, en el aparte 16) "Gestión de incidentes de seguridad de la información", inciso 16.1 "Gestión de incidentes y mejoras en la seguridad de la información" tiene como objetivo "Asegurar que se aplique un enfoque coherente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación de los eventos y debilidades de seguridad"; inciso 16.1.1 "Responsabilidades y procedimientos. Se deben establecer responsabilidades y procedimientos de gestión para asegurarse de tener una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información"; inciso 16.1.2 "Reporte de eventos de seguridad de la información. Los eventos de seguridad de la información deben ser reportados a través de canales de gestión adecuados tan pronto como sea posible".

2.12. En el inciso 16.1.3 "Reporte de debilidades de seguridad de la información. Los empleados y contratistas que utilizan los sistemas y servicios de información de la organización deben estar obligados a notar y reportar cualquier debilidad observada o sospechosa de la

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

seguridad de la información en los sistemas o servicios."; inciso 16.1.4. "Evaluación y decisión sobre los eventos de seguridad de la información. Los eventos de seguridad de la información deben ser evaluados y se debe decidir si serán clasificados como incidentes de seguridad de la información."; inciso 16.1.5 "Respuesta a incidentes de seguridad de la información. Se deben responder los incidentes de seguridad de la información de acuerdo con los procedimientos documentados."; inciso 16.1.6. "Aprendiendo de los incidentes de seguridad información. El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe ser utilizado para reducir la posibilidad o el impacto de incidentes en el futuro."; inciso 16.1.7. "Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recopilación, adquisición y preservación de la información, que puede servir como evidencia."

2.13. Cobit 5 (ISACA 2012), indica en su proceso DSS02 "Gestionar Peticiones e Incidentes de Servicio. Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes."; DSS02.01 "Definir esquemas de clasificación de incidentes y peticiones de servicio. Definir y comunicar la naturaleza y las características de los potenciales incidentes relacionados con seguridad para que puedan ser fácilmente reconocidos y su impacto entendido y, así, permitir una respuesta adecuada."; DSS02.02 "Registrar, clasificar y priorizar peticiones e incidentes. Identificar, registrar y clasificar peticiones de servicio e incidentes, y asignar una prioridad según la criticidad del negocio y los acuerdos de servicio."

2.14. En el DSS02.03 "Verificar, aprobar y resolver peticiones de servicio. Seleccionar los procedimientos adecuados para peticiones y verificar que las peticiones de servicio cumplen los criterios de petición definidos."; DSS02.04 "Investigar, diagnosticar y localizar incidentes. Identificar y registrar síntomas de incidentes, determinar posibles causas y asignar recursos a su resolución."; DSS02.05 "Resolver y recuperarse ante incidentes. Documentar, solicitar y probar las soluciones identificadas o temporales y ejecutar acciones de recuperación para restaurar el servicio TI relacionado."; DSS02.06 "Cerrar peticiones de servicio e incidentes. Verificar la satisfactoria resolución de incidentes y/o satisfactorio cumplimiento de peticiones, y cierre."

2.15. Por su parte Cobit 5, en el proceso BAI09, indica que se debe mantener la resiliencia de los activos críticos mediante la aplicación de un mantenimiento preventivo regular, de supervisión del rendimiento y, si fuera necesario, proporcionando alternativas y/o activos adicionales para reducir la probabilidad de fallo. Adicionalmente, refiere al establecimiento de un plan de mantenimiento preventivo para todo el hardware, considerando un análisis costo beneficio, recomendaciones del proveedor, el riesgo de interrupción del servicio, personal cualificado y otros factores relevantes.

2.16. En relación con la gestión de configuraciones, el proceso BAI010 de Cobit 5 establece la importancia de definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información asociada con la configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.

2.17. En materia de gobierno y gestión de TI, el MEIC cuenta con una planificación estratégica de TI que guarda relación con el plan estratégico institucional. No obstante, el MEIC no ha definido ni aprobado su "Marco de gobierno y gestión de tecnologías de información", que considere aspectos como la gobernanza de TI, la naturaleza, complejidad, tamaño, modelo

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

de negocio, volumen de operaciones, criticidad de sus procesos, riesgos y grado de dependencia en las tecnologías; y que permita la alineación entre las expectativas del negocio y los objetivos estratégicos de tecnologías de información.

2.18. Asimismo, en relación con la estructura en TI, se observó que si bien existe el Comité Gerencial de TI como instancia técnica entre el máximo jerarca del MEIC y la Unidad Informática, el cual reúne personal del área técnica y personal del negocio, y es el encargado de asesorar al máximo jerarca en lo relativo a direccionamiento de proyectos, particularmente en cuanto al uso de los recursos humanos, materiales y financieros que se destinen para su desarrollo; en lo que respecta a su integración, este es presidido por un colaborador del área de TIC, así designado como representante del máximo jerarca, que no posee un nivel de jerarquía o gerencia, ni responsabilidades o condición de coordinación[1]; en ese sentido, no se observa, en la revisión de actas[2] que se realizó, que los viceministros o los directores de las líneas de negocio con su conocimiento y competencia sobre estrategia guíen al equipo de TIC, por lo que se ve comprometido el direccionamiento y valor estratégico.

2.19. En relación con los controles establecidos e implementados por el MEIC para gestionar las tecnologías de información, se evidenció que se implementan acciones aisladas por parte del Departamento de TI tales como segmentación de redes, cifrado de datos, algunas prácticas de fortalecimiento de servidores, bitácoras, respaldos periódicos de información, entre otros, sin embargo, como se indicó antes no se ha establecido un modelo de gobernanza tal y como lo sugieren las mejores prácticas; asimismo, al no existir un marco de gobierno y gestión de TI, ni involucramiento de personal estratégico con una visión general del negocio de la institución; dichos controles no se encuentran alineados con objetivos de gobierno que den dirección y organización, ni con la estructura organizacional en TI, y presentan las siguientes debilidades desde el punto de vista de proceso de TI:

Gestión de servicios de TI (Mesa de ayuda): El MEIC no ha formalizado la política y los procedimientos de mesa de ayuda, además de eso, si bien existe la plataforma GLPI[3] para recibir las solicitudes de los usuarios, en la práctica los requerimientos ingresan por medios adicionales a esta plataforma, como por ejemplo por correo electrónico, por llamadas telefónicas y de forma presencial, lo que dificulta priorizar y atender los requerimientos del usuario y las incidencias de seguridad.

Gestión de incidentes y problemas: además de la debilidad indicada en el punto anterior, en relación con los diversos medios por los cuales se reciben las solicitudes de los usuarios, lo que ocasiona el registro parcial en la plataforma GLPI, se presenta la debilidad en relación con el diseño del proceso de gestión de incidentes y problemas, debido a que no se realiza la separación operativa de dichas solicitudes, independientemente del medio por el cual se reciben, para determinar lo que se considera un *requerimiento de servicio*, cuya finalidad es obtener información, un producto o soporte técnico, respecto de lo que se considera propiamente como *incidente*, por lo que el procedimiento para ambos casos es el mismo. En ese sentido, no se han definido criterios para declarar un evento, incidente o

[1] Plan de Seguridad 2022 V4. "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información" Directriz N°001-MEIC-2021.

[2] En atención al Informe de la Auditoría de Carácter Especial sobre la gestión de los sistemas de información en el MEIC, con referencia DFOE-EC-IF-17-2015.

[3] Conjunto de políticas, procedimientos, organización (roles y responsabilidades), equipos de trabajo, liderazgo, cultura, infraestructura tecnológica, operaciones, y modelo de evaluación y mejora que es administrado por un gestor de seguridad (oficial de seguridad) para garantizar razonablemente la protección de los activos.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

desastre; y se carece de una clasificación de los incidentes, que considere su categorización, impacto, y prioridad.

Gestión de cambios: Se evidencia que existe un procedimiento para la administración de cambios, sin embargo, a la fecha no se cuenta con un comité de cambios que integre al negocio con TI, en el esfuerzo por determinar qué asuntos deben ser considerados y priorizados como cambios y qué asuntos deben esperar o ser descartados. Por lo anterior, se omite la participación del negocio en el análisis de las solicitudes de variación a los sistemas y esas solicitudes solo pasan por revisión del personal de tecnologías de información. No se gestiona mediante mesa de ayuda, ni existe ambiente de pruebas, sino que sólo se ejecutan y se publican. Adicionalmente, no existen procesos formalmente establecidos que permita analizar si existen numerosos cambios de la misma naturaleza, consensuar el contenido de las versiones, acordar las fases y tiempos en que se pondrá a disposición del usuario, recursos necesarios, roles y responsabilidades, el diseño, construcción y configuración de la versión, hasta su distribución e implementación. Aunado a lo indicado, en el MEIC no existe una asignación de prioridad de las solicitudes de cambio, que considere, al menos, la evaluación del impacto y urgencia del cambio.

Mantenimiento preventivo y correctivo: Si bien se encontró evidencia de que se realizan mantenimientos a un conjunto de elementos que hacen parte de la infraestructura tecnológica, no se evidencia que estos mantenimientos obedezcan a una estrategia o a un calendario trazado previamente que contemple todos los elementos que deben recibir el respectivo mantenimiento y su prioridad en relación con el aporte para el cumplimiento de los objetivos institucionales, esto es particularmente aplicable en el caso de equipos de usuario final. En general, no fue posible determinar si todos los equipos que deben recibir mantenimiento finalmente lo reciben en tiempo y forma.

Gestión de Versiones y de Configuraciones: En el MEIC no existen procedimientos formalmente establecidos, para la identificación, control, mantenimiento y verificación de los elementos de configuración de la infraestructura de tecnologías de información, esto incluye la base de datos donde se almacenan dichos elementos y su interrelación (llamada CMDB), la misma toma la forma de un inventario de equipos, por lo que cumple parcialmente con su cometido. En consecuencia, el departamento que administra las tecnologías de información no cuenta con información completa y confiable sobre la infraestructura con la que entregan servicios.

2.20. La falta de un marco de gobierno y gestión de las tecnologías de información como herramienta para alcanzar la alineación entre las expectativas del negocio y los objetivos estratégicos de tecnologías de información, obedece a la limitada participación de los jerarcas y líderes del negocio en el Comité Gerencial de TI, el cual debe funcionar como un órgano de nivel estratégico que vela por el cumplimiento de los objetivos de negocio soportados por TI, y que orienta a los equipos en la ejecución de proyectos y en la implementación de controles para garantizar que se satisfacen las necesidades de diferentes partes interesadas, incluyendo el despacho.

2.21. Toda vez que el departamento de TI debe atender los procesos sin el direccionamiento de parte del negocio se enfrenta a dificultades que tienen que ver con la correcta asignación de recursos, y con la definición de aquello que se espera del área técnica. Las políticas y procedimientos que suelen normar procesos clave de TI están pendientes de elaboración por cuanto el llamado a liderar, que es el órgano de mayor nivel jerárquico no ha direccionado para la ejecución de dicha tarea; observándose que los avances que se han alcanzando en este particular resultan exclusivamente del esfuerzo del equipo de ingeniería.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.22. El Marco de Gobierno y Gestión es un modelo que permite articular los procesos de TI y unirlos a los procesos de negocio. Facilita la prestación de servicios y orienta la labor del departamento de TI en todos los ámbitos de la técnica, por eso, la falta de definición en esta materia incide en la toma de decisiones y en las capacidades y cobertura que presenta el área técnica. Afecta a todos los procesos de TI del MEIC y por ende los principios básicos de seguridad y pone en riesgo el cumplimiento de los objetivos estratégicos tanto de TI como del negocio.

2.23. Las deficiencias en los procesos de TI podrían incrementar el riesgo de que las modificaciones implementadas en los programas, tareas, configuraciones o parámetros de los activos de TI, la afectación por ocurrencia de incidencias, o la falta de mantenimiento por ejemplo, provoquen un impacto adverso a la infraestructura de tecnologías de información existente y con ello se comprometa la confidencialidad, integridad y disponibilidad de los activos de información. Puede incidir en la capacidad operativa del Departamento de Tecnologías de Información (DTI) para la prestación de servicios, con la consecuente afectación a los usuarios de los servicios de TI. La calidad, oportunidad y continuidad de la prestación de los servicios que brinda el MEIC está directamente relacionada con los procesos ejecutados por TI para soportar los sistemas.

2.24. Entendiendo al SIEC como un sistema de misión crítica que hace parte de un conjunto de sistemas operados y soportados por TI, cualquiera de los riesgos de seguridad que se manifiestan por debilidades en los controles implementados por TI, son aplicables a la infraestructura tecnológica en general y son de aplicación para el SIEC así como para el proceso de negocio que se sustenta en dicho sistema.

Ausencia de un Sistema de Gestión de Seguridad de Información (SGSI) en el MEIC

2.25. El sistema de gestión de seguridad de la información es un conjunto de políticas, procedimientos, estándares, directrices, prácticas, y demás lineamientos que tienen por objeto garantizar la protección de los activos de información en línea con los requerimientos y la estrategia del negocio.

Debilidades relacionadas con el sistema de gestión de seguridad de la información (SGSI) en el MEIC

2.26. Cobit 5 en la práctica de gestión APO01.03 Mantener los elementos catalizadores del sistema de gestión, en la actividad 4 recomienda “Alinear el entorno de control de TI con el entorno de políticas de TI, con los marcos de trabajo generales de gobierno de TI y procesos de TI y los marcos de trabajo existentes a nivel corporativo en cuanto a riesgo y control. Evaluar las buenas prácticas o los requisitos específicos del sector (p. ej., normativa específica del sector) e integrarlos donde corresponda.

2.27. Además la práctica APO01.04 establece la necesidad de “Comunicar los objetivos y la dirección de gestión” en su actividad 1 indica “Comunicar continuamente los objetivos y la dirección de TI. Asegurar que las comunicaciones reciban apoyo de la dirección ejecutiva, tanto de palabra como mediante acciones, empleando todos los canales disponibles” y la actividad 2 plantea “Garantizar que la información comunicada engloba una clara articulación de la misión, los objetivos de servicio, la seguridad, los controles internos, la calidad, el código ético/de conducta, las políticas y procedimientos, los roles y las responsabilidades, etc. Comunicar la información con el nivel de detalle adecuado para cada respectiva audiencia dentro de la empresa”.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.28. En su proceso APO13 desde la práctica 1 Cobit 5 señala la necesidad de "Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que estén alineados con los requerimientos de negocio y la gestión de seguridad en la empresa"; para lo cual deberá "Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología.", según detalla la actividad APO13.01.01.

2.29. La norma ISO 27001:2013 señala en el inciso 4.4 sobre el SGSI que "La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta norma internacional", además en el 5.1 se indica que "la alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información:

a) asegurando que *se establecen la política y los objetivos de seguridad* de la información y que estos sean compatibles con la dirección estratégica de la organización (...) c) asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles (...) f) dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información (...)."

2.30. En lo que respecta a la clasificación de información, Cobit 5 señala en la práctica APO01.06 que se debe "Definir y mantener las responsabilidades de la propiedad de la información" (datos) y los sistemas de información. Asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación." En ese sentido, la primera actividad que se señala es "Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información (datos) en toda la empresa".

2.31. El proceso DSS04 de Cobit 5 se refiere en su totalidad al proceso de gestión de la continuidad y establece como primera práctica la necesidad de "Definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes

2.32. interesadas" para luego desarrollar y mantener la estrategia de continuidad en su práctica 02. Se define en la práctica de gestión 03 que se debe "Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas".

2.33. Por otro lado el mismo DSS04 señala en su práctica 04 que se debería "Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera", esto incluye entre otras cosas; "Definir los objetivos para ejercitar y probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio (BCP), para enfrentarse a los riesgos de negocio" así como "Definir y acordar ejercicios que sean razonables con las partes interesadas, validar los procedimientos de continuidad, e incluir roles y responsabilidades y acuerdos de retención de datos que ocasionen la mínima disrupción en los procesos de negocio".

2.34. Cobit 5 en su proceso DSS01 sobre gestión de operaciones en la práctica DSS01.01 que se debe "Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados" y se debe "Mantener una programación de actividades operativas, ejecutar las actividades y gestionar el desempeño y rendimiento

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

(throughput) de las actividades programadas" así como "Programar, realizar y registrar las copias de respaldo de acuerdo con las políticas y procedimientos establecidos".

2.35. En esa línea la norma ISO 27002 en su apartado 10.5 sobre respaldos establece que "Se debería establecer procedimientos de rutina para implementar una política y estrategia acordada de respaldo (…) haciendo copias de respaldo de datos y ensayando su oportuna restauración". Entre otras cosas se señala que "se debería producir procedimientos documentados de restauración y registros exactos y completos de las copias de respaldo" y en el inciso f de la guía de implementación se amplía "los medios de respaldo se deberían probar regularmente para asegurarse que pueden ser confiables para el uso cuando ser necesarios".

2.36. ISO 27001 en el enunciado de control A.7.2.2 establece que "todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo".

2.37. ISO 27002 aparte 8.2.2 define el control de la siguiente manera "Todos los empleados de la organización y, donde sea pertinente, contratistas y usuarios de terceras partes deberían recibir formación adecuada en toma de conciencia y actualizaciones regulares en políticas y procedimientos organizacionales, pertinentes para su función laboral". Además se señala que "La formación en toma de conciencia debería comenzar con un proceso de inducción formal ideado para introducir las políticas y expectativas de la organización antes de otorgar acceso a información o servicios".

2.38. En cuanto a las buenas prácticas internacionales contenidas en el proceso DSS05, denominada "Gestionar los Servicios de Seguridad" del COBIT 5, señala la necesidad de "proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad". Este proceso especifica que se deben llevar a cabo, entre otras, las siguientes actividades: "mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados."

2.39. Tal como lo indica la Norma ISO 27001:2014 en su aparte A.9.4 "Control de acceso a sistemas y aplicaciones", cuyo objetivo es prevenir el acceso no autorizado a los sistemas y aplicaciones específicamente en el control, A.9.4.1 Restricción del acceso a la información, se "Deberá restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida".

2.40. La misma norma en su inciso A.9.4.4 sobre el uso de utilidades con privilegios de sistema señala que se debe "Restringir y controlar rigurosamente el uso de utilidades que pueda ser capaces de invalidar los controles del sistema y de la aplicación".

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.41. Estos conceptos se refuerzan en la norma ISO 27002 en el aparte 11.2 sobre gestión de acceso de usuario donde se plantea que "Se debería tener especial atención, cuando corresponda, a la necesidad de controlar la asignación de derechos de acceso privilegiados, que permiten a los usuarios anular controles del sistema".

2.42. El apartado 11.2.2 de la citada norma trata la gestión de privilegios y hace una salvedad importante en el caso de usuarios privilegiados en el inciso f "los privilegios deberían ser asignados a una identificación de usuario (ID) diferente de la utilizada para uso normal del negocio" esto es consistente con el señalamiento sobre usuarios genéricos que no tienen una justificación expresa del negocio para estar activos.

2.43. En cuanto a los ejercicios de escaneo de vulnerabilidades, estos pueden realizarse de manera automatizada, de manera manual o en una combinación, pueden realizarse internamente o con colaboración de terceros. En ese sentido se encuentra un apartado en la norma ISO 27002 numeral 12.6 sobre gestión de vulnerabilidades técnicas, se indica que "La gestión de vulnerabilidades técnicas se debería implementar de una manera eficaz, sistemática, y repetible con toma de mediciones para confirmar su eficacia. Estas consideraciones deberían incluir los sistemas operativos, y cualquier otra aplicación en uso".

2.44. Se define el control en el numeral 12.6.1 "Se debería obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluarse la exposición de la organización a tales vulnerabilidades, y tomar medidas apropiadas para gestionar el riesgo asociado".

2.45. En la guía de implementación se encuentra en el inciso d la siguiente referencia "una vez que ha sido detectada una potencial vulnerabilidad técnica, la organización debería identificar los riesgos asociados y las acciones a ser tomadas; tal acción podría implicar el instalar el parche a sistemas vulnerables y/o la aplicación de otros controles".

2.46. En el ámbito de seguridad de la información, el MEIC ha tomado acciones[4] para implementar una Política de Seguridad de Información[5] no obstante, se evidenció que a la fecha el MEIC no ha definido un sistema de gestión de seguridad de la información (SGSI) según lo requieren las buenas prácticas en la materia, con sus diferentes componentes[6]. De esta forma, si bien se han implementado medidas de control a nivel de ciberseguridad para sustentar la confidencialidad, la integridad y la disponibilidad de la información, tales como, controles generales a nivel de red, se implementaron reglas para el tráfico de paquetes por medio del firewall, se implementa un sistema antivirus y se mantiene actualizado, se automatizan actualizaciones de sistemas operativos, entre otros; estas han ocurrido de manera reactiva y en función de las circunstancias al momento que van surgiendo, y no en atención a un sistema de gestión de seguridad de información.

2.47. En ese contexto, se evidenció la inexistencia de políticas, procedimientos y planes complementarios a la Política de Seguridad de Información, y que son relevantes para asegurar la salvaguarda de los activos de información, tal como se detalla de seguido:

[4] Manual para crear un incidente en el Sistema de Control de Incidencias – GLPI.

[5] Artículo 6 del Reglamento de Servicio del Comité Gerencial de Informática del Ministerio de Economía, Industria y Comercio, formalizado mediante Decreto 33628-MEIC, publicado en La Gaceta del 19 de marzo de 2007.

[6] Actas del Comité Gerencial de TI suministradas para el periodo 2019-2021 (19 documentos)

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Se determinó la ausencia de la política y procedimientos para clasificar la información y los sistemas que soportan a nivel institucional. Esta clasificación de información es la base para establecer criticidad de los recursos y en consecuencia aplicar mecanismos de control acordes con la percepción de importancia relativa.

El MEIC no evidenció haber desarrollado un Plan de Continuidad de Negocio que se apoye en un Análisis de Impacto de Negocio (con el visto bueno de los gerentes de línea y los líderes de los procesos que integran las actividades críticas del MEIC). Por ende no existe una definición de lo que harán los equipos de negocio en caso de entrar en contingencia. Actualmente, el MEIC aborda directamente el proceso de recuperación tecnológica por medio de un DRP, el cual fue elaborado por el área técnica, sin participar los gerentes del negocio. En ese sentido al realizar los cálculos de indicadores base como RPO, RTO, MTD se sigue el criterio de ingeniería solamente. En consecuencia, la recuperación considera solamente los procesos de TI, omitiendo, de momento, los procesos de negocio. Aunado a lo expuesto, no se han realizado y documentado pruebas al Plan de Recuperación en caso de Desastre, tales como lista de verificación, prueba de escritorio, simulaciones, paralelo, o interrupción completa en concordancia con lo que se recomienda en las buenas prácticas.

Se determinó la ausencia de una política de respaldo y recuperación, que muestre la dirección que la administración le dará a este proceso, que es crítico para garantizar la continuidad del negocio respecto de bases de datos y computación de usuarios finales. Se encuentra que para el respaldo de bases de datos se cuenta con una programación que establece el tipo de respaldo y la frecuencia, sin embargo se evidencia que no se conoce el universo total de las bases de datos. Asimismo, esta programación no obedece a una valoración de riesgo, a un criterio de negocio que justifique las estrategias implementadas. Por otro lado, se encontró que no se realizan pruebas a los respaldos y tampoco se cuenta con un entorno específico para realizar dicha tarea. Control que resulta necesario para garantizar que los respaldos son confiables para el uso cuando sean necesarios efectivamente completos y utilizables.

No se evidenció el establecimiento de un programa de formación en materia de seguridad de la información, que permita desarrollar un ambiente seguro en lo que a ciberespacio y seguridad de información se refiere, y que cubra a toda la institución, con materiales elaborados para atender las diferentes audiencias o públicos que hacen parte de la organización, así como de las entidades proveedoras de bienes y servicios. Si bien existen algunas acciones orientadas a la sensibilización o cultura de seguridad, estas han sido aisladas y se enfocaron en el personal especializado en TI, por lo cual esta práctica no alcanza a los demás departamentos.

2.48. Además, en relación con las pruebas realizadas sobre el proceso de gestión de identidades (administración de cuentas de usuario), mediante las cuales se analizaron los controles implementados para supervisar las actividades que realizan los usuarios, se determinó las siguientes debilidades:

Se identificaron 173 cuentas de naturaleza genérica en el gestor de cuentas conocido como Active Directory (software que implementa Windows a nivel de servidor para centralizar la administración de roles y perfiles), las cuales no se encuentran documentadas a nivel de negocio. Algunas de estas cuentas son de tipo “admin” y cumplen un rol general en la administración de aplicaciones por ejemplo el antivirus, o el firewall. Estas cuentas no tienen asignado un responsable por su uso, lo cual resulta inadecuado desde el punto de vista de gestión de seguridad.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Además se localizan 2 cuentas de usuario (que vienen del sistema CRM) que han dejado la institución y permanecen activas en el AD.

En el caso de personal que se ausenta de su cargo de manera justificada por un periodo de tiempo extenso y conocido, por ejemplo en la aplicación de permisos sin goce de salario que superan el plazo de un año, los usuarios permanecen activos en el AD, cuando deberían estar en estado de suspendidos durante ese tiempo a la espera de su retorno a la institución.

No se han diseñado e implementado controles específicos para supervisar el desempeño y las actividades que realizan los usuarios privilegiados, si bien existen bitácoras, esto no es suficiente para asegurar que las actividades realizadas por estos usuarios son conocidas y aprobadas por una persona con autoridad para tal efecto. De la misma forma no se evidenció el ejercicio de supervisión directa sobre las actividades que desempeñan los usuarios finales.

2.49. Particularmente, en relación con la seguridad del SIEC, se determinó que presenta debilidades significativas que van desde la versión del sistema que se maneja hoy en el SIEC, así como la estabilidad y respaldo del sistema operativo y sus actualizaciones. Se suma a estas debilidades la posibilidad que tienen otros usuarios con roles distintos al de Administrador, de borrar o modificar campos. Además la ausencia de validación externa de los datos ingresados por el solicitante, y de alguna declaración jurada para dar validez a los datos ingresados al sistema. Por otro lado, desde el punto de vista de implementación, el sistema cuenta con un modelo de autenticación de un solo factor (usuario y contraseña), además carece de controles que previenen los ataques de denegación de servicio como el uso de un captcha.

2.50. Asimismo, los controles de entrada de datos dejan pasar gran cantidad de espacios en blanco. Las máscaras de entrada de datos no son efectivas y no manejan mensajes de error apropiados para guiar al usuario. Los informes no son parametrizables, y no se pueden exportar a un formato que facilite su procesamiento de manera integral.

2.51. Adicionalmente, se desarrolló una batería de pruebas manuales con el fin de detectar vulnerabilidades en el entorno web tanto del MEIC como del SIEC. El resultado de estas pruebas es confidencial dada la sensibilidad de los hallazgos, por lo que se remitió oficio con el detalle de las mismas y en carácter confidencial al ministerio con el propósito de que realizara valoración de las situaciones identificadas y definiera la procedencia de implementar medidas y controles de seguridad.

2.52. El MEIC no cuenta con un sistema de gestión de seguridad de la información, debido a que no ha establecido un proceso para la definición e implementación de dicho SGSI; en consecuencia, la Política de Seguridad de Información, no se estableció como parte de un conjunto de herramientas, controles, técnicas, actividades y motivaciones que son entradas sugeridas por las buenas prácticas, tales como Cobit 5 para seguridad, el marco NIST o la norma ISO 27001. De esa forma, a la fecha el MEIC no ha adoptado un marco de gestión de seguridad particular, tampoco tiene conocimiento de las brechas que existen en su postura de seguridad con respecto a dicho marco, no ha definido el alcance y los límites del sistema de gestión de seguridad de la información (SGSI), y no ha abordado una estrategia institucional, que permita definir la postura de seguridad deseada y establecer las acciones así como los responsables para alcanzarla en un plazo predefinido.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.53. La falta de orientación en materia de seguridad de información, alineada con los objetivos institucionales, tiene efectos adversos sobre la confidencialidad, la disponibilidad y la integridad de la información, es decir, se compromete todo esfuerzo de la administración para proteger sus activos dado que no se conocen los escenarios de riesgos a los que se enfrenta el equipo de TI y la organización como un todo. Dado que la estrategia de seguridad resguarda todos los sistemas que hacen parte de la infraestructura tecnológica, el SIEC no escapa de esa realidad y en tanto se ausentan controles relevantes como los propios de continuidad de negocio, gestión de identidades y vulnerabilidades conocidas a nivel web, son todos asuntos que inciden sobre la seguridad del principal sistema que utiliza DIGEPYME.

2.54. La ausencia de planes de continuidad de negocio tiene un impacto directo sobre la disponibilidad de los sistemas de misión crítica. Cuando no se determinan los umbrales de recuperación adecuadamente, puede ser que se utilicen recursos de forma ineficiente y se exponga la infraestructura a pérdidas de datos que pueden ir más allá de lo tolerable.

2.55. Las deficiencias en materia de seguridad lógica pueden tener un impacto sobre la confidencialidad y la disponibilidad de la información y los sistemas. Suelen asociarse con la posibilidad de dejar abiertos portillos que pueden ser explotados por un atacante. Por ejemplo, el uso de usuarios genéricos no controlados podría facilitar la escalación de privilegios en la red o el acceso no autorizado si se combina con otras vulnerabilidades en el entorno web.

3. Conclusiones

3.1. En atención a los principios de seguridad, de confidencialidad e integridad, se encuentra que el MEIC presenta importantes debilidades en materia de seguridad lógica y ciberseguridad, por ende no se cumple razonablemente con las mejores prácticas en la materia ni con lo establecido en el marco técnico que le es aplicable.

3.2. La ausencia de un marco de gobierno y gestión de TI y de una estrategia para implementar el sistema de gestión de seguridad de información inciden negativamente sobre los controles implementados por TI a nivel de operaciones, esto incluye entre otras cosas la emisión y debida formalización de políticas y procedimientos así como en el diseño e implementación de controles clave en materia de ciberseguridad y de seguridad de información.

3.3. Los procesos implementados por el negocio y por TI no brindan una garantía de continuidad del servicio, es decir, ante un evento disruptivo no se han desarrollado e implementado los mecanismos de respuesta que permitan al negocio continuar con la operación en un esquema de contingencia.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

4. Disposiciones

4.1. De conformidad con las competencias asignadas en los artículos 183 y 184 de la Constitución Política, los artículos 12 y 21 de la Ley Orgánica de la Contraloría General de la República, Nro. 7428, y el artículo 12 inciso c) de la Ley General de Control Interno, se emiten las siguientes disposiciones, las cuales son de acatamiento obligatorio y deberán ser cumplidas dentro del plazo (o en el término) conferido para ello, por lo que su incumplimiento no justificado constituye causal de responsabilidad.

4.2. Para la atención de las disposiciones incorporadas en este informe deberán observarse los "Lineamientos generales para el cumplimiento de las disposiciones y recomendaciones emitidas por la Contraloría General de la República en sus informes de auditoría", emitidos mediante resolución Nro. R-DC-144-2015, publicados en La Gaceta Nro. 242 del 14 de diciembre del 2015, los cuales entraron en vigencia desde el 4 de enero de 2016

4.3. Este órgano contralor se reserva la posibilidad de verificar, por los medios que considere pertinentes, la efectiva implementación de las disposiciones emitidas, así como de valorar el establecimiento de las responsabilidades que correspondan, en caso de incumplimiento injustificado de tales disposiciones.

AL SR. FRANCISCO GAMBOA SOTO EN SU CALIDAD DE MINISTRO DE ECONOMÍA INDUSTRIA Y COMERCIO O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. Declarar, aprobar y divulgar el marco de gobierno y gestión de TI que utilizará el MEIC en adelante. Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General una certificación que haga constar que, al 30 de enero de 2023, se declaró, aprobó y divulgó el marco de gobierno y gestión de TI. (ver párrafos del 2.17 al 2.24).

4.5. Resolver con respecto a la propuesta de proceso de implementación gradual que presente el comité de TI. Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General, a más tardar el 30 de mayo de 2023, una certificación que acredite que se resolvió con respecto al proceso de implementación gradual de cada uno de los componentes del marco de gobierno y gestión de TI (ver párrafos del 2.17 al 2.24).

4.6. Declarar y divulgar el marco de seguridad de información que utilizará el MEIC en adelante. Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General una certificación, a más tardar el 30 de enero de 2023, en la que conste que se declaró y divulgó el marco de seguridad de información. (ver párrafos del 2.46 al 2.55).

4.7. Resolver con respecto a la propuesta de hoja de ruta para la implementación gradual del Sistema de Gestión de Seguridad de Información. Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General, una certificación, a más tardar el 30 de junio de 2023, en la que conste lo resuelto con respecto a la hoja de ruta para la implementación del Sistema de Gestión de Seguridad de Información. (ver párrafos del 2.46 al 2.55).

4.8. Resolver con respecto a la propuesta para la atención inmediata de las vulnerabilidades críticas, así como, en relación con la hoja de ruta para atender las vulnerabilidades clasificadas como intermedias o de bajo riesgo, que presente el comité de TI. Para dar cumplimiento a esta disposición deberá remitirse a la Contraloría General, a más tardar el 28

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

de febrero de 2023, una certificación que acredite que se resolvió con respecto a la propuesta y la hoja de ruta. (ver párrafo del 2.51).

4.9. Elaborar, aprobar, y comunicar una Política de Continuidad de Negocio y un Análisis de Impacto de Negocio (BIA) que sirva como insumo al proceso de continuidad de negocio y contingencia tecnológica en el cual se definan los umbrales de riesgo aceptables, así como los indicadores que sustentan los planes entre otros RPO, RTO, MTO, etc. Este documento debe tener un alcance institucional y cubrir todos los procesos de negocio y los sistemas que lo soportan.

Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General, una certificación que haga constar que, al 28 de febrero de 2023, se elaboró, aprobó y comunicó a las partes interesadas el Análisis de Impacto de Negocio (BIA), una certificación que haga constar que, al 31 de marzo de 2023, se elaboró, aprobó y comunicó a las partes interesadas la Política de Continuidad de Negocio. (Ver párrafos 2.46 al 2.55).

AL COMITÉ GERENCIAL DE INFORMÁTICA DEL MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMERCIO

4.10. Diseñar y enviar a aprobación del jerarca una propuesta de proceso de implementación gradual del marco de gobierno y gestión de tecnologías de información, que considere la valoración de brechas para comprender el estado actual del gobierno y la gestión de TI con respecto a dicho marco; que contemple los procesos de gobierno y gestión de tecnologías de TI, y que atienda las debilidades señaladas en los párrafos del 2.16 al 2.23. En dicho proceso deberá definirse la periodicidad y el responsable de rendir al Ministro informes de avance. Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General, a más tardar el 31 de marzo de 2023 una certificación que haga constar que se diseñó y envió al Jerarca la propuesta de implementación del marco de gobierno y gestión de TI, y que como parte de ese proceso se definió la periodicidad y el responsable de rendir al Ministro informes de avance sobre la ejecución del proceso de implementación gradual del marco de gobierno y gestión de TI. (ver párrafos del 2.17 al 2.24).

4.11. Diseñar y enviar a aprobación del jerarca una hoja de ruta para la implementación del Sistema de Gestión de Seguridad de Información, que incluya al menos, fechas estimadas de inicio y finalización, las actividades o tareas a realizar y sus respectivos responsables; además, deberá considerar la valoración de brechas para comprender el estado actual de la seguridad de la información del Ministerio y el estado de seguridad deseado por la institución en el mediano y largo plazo; el alcance y los límites del SGSI en términos de las características del MEIC, activos y tecnología. Además, definir la periodicidad y el responsable de rendir al Ministro informes de avance.

Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General, una certificación que haga constar que, al 28 abril de 2023, se diseñó y envió a aprobación del Jerarca, la hoja de ruta para la implementación gradual del SGSI. Además, remitir al Órgano Contralor tres informes con periodicidad trimestral en fechas 31 de julio 2023, 31 de octubre 2023 y 31 de enero 2024 sobre el avance de la implementación de dicha hoja de ruta, en el que se indique el grado de avance, las actividades pendientes y las fechas estimadas para cerrar dichos pendientes. (ver párrafos del 2.46 al 2.55).

4.12. Diseñar, aprobar, comunicar e implementar un programa de sensibilización en materia de seguridad de información que cubra a todo el MEIC y que atienda a usuarios específicos y sus necesidades. Al respecto se deberá elaborar el material respectivo, ejecutar el programa de sensibilización y llevar a cabo actividades de reforzamiento en el tiempo para

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

asegurar que el esfuerzo es sostenido. Además las actividades realizadas deberán documentarse adecuadamente.

Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General, una certificación que haga constar que, al 28 de abril de 2023, se diseñó, aprobó, comunicó e inició el programa de sensibilización. Además, al 30 de julio de 2023, remitir al Órgano Contralor un informe en el que se detalle el grado de avance en la implementación y los pendientes así como las actividades programadas para asegurar la sostenibilidad del programa de sensibilización. (ver párrafos del 2.46 al 2.55).

4.13. Diseñar y enviar a aprobación del Jerarca una propuesta para atender de forma inmediata las vulnerabilidades señaladas como críticas y una hoja de ruta para la atención de las vulnerabilidades clasificadas como intermedias o de bajo riesgo en la infraestructura web tanto del SIEC como del MEIC. Para ello, se deberá considerar actividades, responsables, recursos y plazos.

Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General, una certificación que haga constar que, al 31 de enero de 2023, se diseñó y envió a aprobación del Jerarca una propuesta para atender de forma inmediata las vulnerabilidades señaladas como críticas en la infraestructura web tanto del SIEC como del MEIC, y una hoja de ruta para la atención de las vulnerabilidades clasificadas como intermedias o de bajo riesgo. Además, remitir al Órgano Contralor una certificación en fecha 30 de junio 2023 en la que se señale la atención de vulnerabilidades críticas y al 31 de octubre 2023 un informe sobre la implementación de la hoja de ruta, en el que se indique el grado de avance, las actividades pendientes y las fechas estimadas para cerrar dichos pendientes. (ver párrafo 2.51).

Firmado digitalmente por FALON STEPHANY ARIAS CALERO
Fecha: 2022-12-09 13:59

Falon Stephany Arias Calero
Gerente de Área

Firmado digitalmente por MARI TRINIDAD VARGAS ALVAREZ
Fecha: 2022-12-09 14:28

Mari Trinidad Vargas Álvarez
Asistente Técnico

Firmado digitalmente por ALEJANDRO ZUÑIGA GOMEZ
Fecha: 2022-12-09 13:54

Alejandro Zúñiga Gómez
Fiscalizador

Firmado digitalmente por JENNIFER PRISCILLA VILLARREAL SEQUEIRA
Fecha: 2022-12-09 13:55

Jennifer Villarreal Sequeira
Fiscalizadora Asociada

/aam
Ce: Archivo
G: 2022000345-1
Exp: CGR-INAU-2022000407

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica