IPES - Correspondencia Administrativa- INTERNAS
Radicado: 00110-817- 002997
Fecha: 20/05/2020 - 12:08 PM
Remitente: CARMEN ELENA BERNAL ANDRADE
Dependencia: Despacho de la Oficina Asesora de Control Interno
Destinatario: LIBARDO ASPRILLA LARA
Destino: DIRECCION GENERAL
Folios: 2 Anexos: 0

MEMORANDO

110301

Bogotá DC.,

PARA: LIBARDO ASPRILLA LARA, Director General

DE: CARMEN ELENA BERNAL ANDRADE, Asesora de Control Interno

ASUNTO: FUNCION PREVENTIVA ATENCIÓN A LOS CONTROLES DE INFRAESTRUCTURA DE TI PARA LA MITIGACIÓN DE RIESGOS DE SEGURIDAD DIGITAL

Respetado Director,

En el ejercicio de las funciones asignadas a la Asesoría de Control Interno, de manera específica en el rol *"Enfoque hacia la Prevención",* establecido en el artículo 17 del Decreto 648 de 2017 modificatorio del artículo 2.2.21.5.3 del Decreto 1083 de 2015, las Oficinas de Control Interno o quienes hagan sus veces, tienen el deber de formular recomendaciones con alcance preventivo, que le sirvan a la entidad para la toma de decisiones frente al quehacer institucional y su mejora, con el fin de advertir sobre operaciones o procesos en ejecución y prever graves riesgos que comprometan el patrimonio público.

En el mismo sentido, la Circular 01 del 9 de julio de 2015 expedida por el Consejo Asesor del Gobierno Nacional en Materia de Control Interno de las Entidades de Orden Nacional y Territorial, cuyo asunto es el fortalecimiento del Sistema de Control Interno frente a la función preventiva asumida por las Oficinas de Control Interno frente a la aplicación de la Sentencia C-103 de 2015 de la Corte Constitucional que declaró inexequible el numeral 7º del artículo 5º del Decreto Ley 267 de 2000, donde era la Contraloría General de la República quien advertía sobre las operaciones o procesos en ejecución, con el fin de prever graves riesgos que comprometieran el patrimonio público.

En consonancia con lo anterior, la mencionada circular trajo a colación, que el constituyente dispuso de otros mecanismos, como el art. 209 y 269 de la Constitución Política de Colombia, en virtud de los cuales las entidades públicas están obligadas a implementar un sistema de control interno, que pueda intervenir de manera previa, concomitante o posterior para detectar y corregir las desviaciones en la gestión de la entidad, que pueden afectar el cumplimiento de sus objetivos.

Calle 73 N° 11-66
PBX. (+57) 2976030
Línea Gratuita
018000124737
www.ipes.gov.co

De la misma manera, el artículo 12 de la Ley 87 de 1993, que asigna funciones a los Jefes de Control Interno o quienes hagan sus veces, en especial, los siguientes literales:

> *"e) Verificar que los controles definidos para los procesos y actividades de la organización se cumplan por los responsables de su ejecución, (…)*
>
> *d) Verificar que los controles asociados con todas y cada una de las actividades de la organización estén adecuadamente definidos, sean apropiados y se mejoren permanentemente, de acuerdo con la evolución de la entidad; (...)*
>
> *g) Verificar los procesos relacionados con el manejo de los recursos, bienes y los sistemas de información de la entidad y recomendar los correctivos que sean necesarios; (...)"*

Son fundamento de la presente **Función Preventiva,** en ejercicio de los principios de: autocontrol, autogestión y autorregulación, sin llegar a que esta Asesoría de Control Interno autorice ni refrende los procedimientos administrativos del Instituto para la Economía Social - IPES.

Los controles tecnológicos o de infraestructura de TI, deben respaldar y garantizar la continuidad de los diferentes servicios y procesos de la entidad, tales como: redes, bases de datos, sistemas operativos, aplicaciones, software y hardware, entre otros.

He aquí la importancia de la Norma ISO/IEC 27001:2013, este estándar Internacional proporciona un modelo para establecer, implementar, monitorear, revisar y mantener un sistema de gestión de seguridad de la información (SGSI). A partir de lo definido en el Anexo A, normativo y con los controles de seguridad.

ANEXO A NORMA ISO 27001:2013	
	A.5. Política General de Seguridad de la Información
	A.6. Organización de Seguridad de la Información
	A.7. Seguridad de los Recursos Humanos
	A.8. Gestión de Activos
	A.9. Control de Acceso
	A.10. Criptografía
	A.11. Seguridad Física y del Entorno
	A.12. Seguridad de las Operaciones
	A.13. Seguridad de las Comunicaciones
	A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas
	A.15. Relaciones con los Proveedores
	A.16. Gestión de Incidentes de Seguridad de la Información
	A.17. Seguridad de la Información en la Continuidad del Negocio
	A.18. Cumplimiento de Requisitos Legales y Contractuales

Calle 73 N° 11-66
PBX. (+57) 2976030
Línea Gratuita 018000124737
www.ipes.gov.co

La norma ISO 27001:2013 se enfoca en el aseguramiento de la confidencialidad, integridad y disponibilidad de los datos, al igual que de los sistemas que se encargan de gestionar la seguridad de la información. La entidad debe elegir cuales controles son aplicables a sus necesidades, es importante entender que no solo se limita al área TI, sino que también involucra áreas como la administrativa, recursos humanos, financiera, comunicaciones, entre otros.

De acuerdo con lo anterior y entendiendo que del Instituto para la Economía Social – IPES al transcurrir del tiempo ha venido validando e implementando algunos de los controles de la ISO 27001:2013, se hace necesario fortalecer el monitoreo, control y seguimiento en la implementación de estos teniendo en cuenta que de acuerdo a la Guía de Administración de Riesgos y Diseño de Controles (DAFP,2018) adopta este marco de referencia ISO para la Entidades Públicas; más aun teniendo de presente el evento de riesgo ocurrido en el Instituto: indisponibilidad total de los servicios tecnológicos presentada entre los días 13 y 14 de mayo de 2020 que afectó la continuidad de la operación y la atención a la ciudadanía por canales virtuales; servicios administrados por el Proceso de Gestión Seguridad de la Información y Recursos Tecnológicos de la entidad.

Desde esta Asesoría de Control Interno se recomienda emprender acciones de revisión continua, que permitan gestionar los riesgos antes de su materialización para disminuir el impacto y la probabilidad de ocurrencia, así como la aparición de nuevos eventos de riesgo que puedan afectar el desempeño del IPES o de los servicios que presta al ciudadano.

Adicionalmente, se recomienda generar un informe del incidente presentado, las acciones realizadas para mitigar el impacto, las lecciones aprendidas, lo anterior identificando los riesgos y vulnerabilidades a los que se vio expuesta la infraestructura tecnológica.

Por último, es importante destacar que la Asesoría de Control Interno en su rol de "*Evaluación y Seguimiento"* se articula también con el de *"Evaluación de la Gestión del Riesgo",* en la medida que las auditorías internas deben practicarse con un enfoque basado en riesgos. Al respecto, la Guía para la Administración del Riesgo y Diseño de Controles (DAFP, 2018) indica respecto del monitoreo y revisión de los riesgos, a cargo de las Oficinas o Unidades de Control Interno o quienes hagan sus veces en las entidades del Estado, como **Tercera Línea de Defensa:**

> *"...Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. La tercera línea de defensa está conformada por la oficina de control interno o auditoría Interna..."*

Calle 73 N° 11-66
PBX. (+57) 2976030
Línea Gratuita
018000124737
www.ipes.gov.co

En este sentido, y con base en la normatividad aplicable al Instituto, de acuerdo al análisis normativo que fundamenta la presente **Función Preventiva,** desde esta Asesoría de Control Interno se incluirá en los alcances de los Informes y Seguimientos de Ley, así como en el alcance de las auditorías programadas para la vigencia 2020, la evaluación de las medidas adoptadas por la Administración en relación a los incidentes de seguridad digital que hayan afectado a la entidad y también las métricas o indicadores definidos para hacer seguimiento a las medidas de seguridad implementadas para garantizar la continuidad de los servicios prestados a la ciudadanía por parte del Instituto para la Economía Social – IPES, respecto a su gestión para administrar o mitigar los siguientes tipos de riesgos[1]:

Riesgos Operativos: Comprende riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Cordialmente,

CARMEN ELENA BERNAL ANDRADE

Con copia: Dra. Fátima Verónica Quintero Núñez, Subdirectora de Diseño y Análisis Estratégico

	NOMBRE, CARGO O CONTRATO	FIRMA	FECHA
Elaboró	Carlos Humberto Parra – Contratista ACI CPS 1391726/2020	*Original Firmado*	19/05/2020
Aprobó Revisó	Carmen Elena Bernal Andrade - Asesora de Control Interno	*Original Firmado*	
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para firma de la ***Asesora de Control Interno*** del Instituto para la Economía Social IPES.			

[1] (DAFP, 2018). Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.

Calle 73 N° 11-66
PBX. (+57) 2976030
Línea Gratuita
018000124737
www.ipes.gov.co