AudInforma
- a su servicio

Abril 2022 No. 4

En nuestra cuarta edición del año 2022 deseamos compartir con todos los funcionarios de la institución información relevante sobre:

1. Normas de Control Interno aplicables a la Ciberseguridad de los sistemas de Información PANI
2. Técnicas Útiles para redactar riesgos
3. Ética y Probidad: Contenido de la Directriz 20 Prohíbe funcionarios Públicos Dar Recomendaciones a Personas Privadas“

Esperamos que la información compartida sea de interés y contribuya a mejorar y fortalecer las acciones de control interno desarrolladas por cada uno de los funcionarios de la institución en el ejercicio de las labores efectuadas.

Normas de Control Interno aplicables a la Ciberseguridad de los Sistemas de Información del PANI

IMPORTANCIA:
El Patronato Nacional de la Infancia es la entidad rectora en materia de niñez y adolescencia, su interés superior es la Persona Menor de Edad y la protección integral de la familia. En este sentido resulta necesario que la institución gestione las acciones necesarias de control interno para garantizar la seguridad física y lógica de los sistemas de información institucionales, siendo que los mismos contienen datos que por su naturaleza son de carácter confidencial, y por lo tanto requieren ser protegidos de ataques, daños o accesos no autorizados.

A continuación compartimos algunas normas de control relacionadas con la gestión y control de las tecnologías de la información:

Norma 5.9 Tecnologías de Información
El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance. Para ello deben observar la normativa relacionada con las tecnologías de información emitida por la CGR.(*1) En todo caso, deben instaurarse los mecanismos y procedimientos manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información.

(*1) “Normas técnicas para la gestión y el control de las tecnologías de información”, (N-2-2007-CO-DFOE), aprobadas mediante resolución R-CO-26-2007 del 7 de junio de 2007, y publicadas en el Diario Oficial “La Gaceta” N° 119 del 21 de junio de 2007

Continua en la siguiente página

“Normas técnicas para la gestión y el control de las tecnologías de información”, (N-2-2007-CO-DFOE)

Esta normativa establece criterios de control que deben ser observados como parte de la gestión institucional de las TI, el jerarca y los titulares subordinados como responsables de esa gestión deben establecer, mantener, evaluar y perfeccionar ese marco de control de conformidad con lo establecido en la Ley General de Control Interno Nro. 8292.

Además, es importante indicar que esta normativa es acatamiento obligatorio, y su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable. Algunas de las normas relacionadas directamente con la seguridad de los sistemas de información son:

> **1.4 Gestión de la seguridad de la información** La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.

Para esto la institución debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:

1.4.1 Implementación de un marco de seguridad de la información. La organización debe implementar un marco de seguridad de la información, para lo cual debe:

1.4.2 Compromiso del personal con la seguridad de la información. El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.

1.4.3 Seguridad física y ambiental. La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos.

1.4.4 Seguridad en las operaciones y comunicaciones. La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información.

1.4.5 Control de acceso. La organización debe proteger la información de accesos no autorizados.

1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica. La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información.

1.4.7 Continuidad de los servicios de TI. La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios

TÉCNICAS ÚTILES PARA REDACTAR RIESGOS:

Las Normas de control interno para el Sector Público ***(1)*** definen *RIESGO* como:

> ***"Probabilidad de que ocurran eventos de origen interno o externo, que tendrían consecuencias sobre el cumplimiento de los objetivos institucionales."***

La comprensión del termino es esencial, dado que una de las mayores limitantes dentro del proceso de gestión de riesgos es la falta de un entendimiento común del significado del riesgo.

Además, los riesgos pueden documentarse a través de una gran variedad de formatos, no obstante estas descripciones podrían no estar claras para todas las partes relacionadas con el proceso de administración de riesgos, tendiéndose a confundir en algunas ocasiones causa y efecto.

Es por esto que un paso relevante en el proceso de análisis de riesgos, lo representa el redactar los riesgos en una forma consistente y crear un lenguaje común para toda la organización.

(1)Normas de Control Interno para el Sector Público N-2-2009-CO-DFOE

A continuación se enumeran algunas técnicas de redacción muy efectivas a la hora de redactar riesgos:

Escribir los riesgos en formato de causa y efecto.
Es decir iniciar la definición con una breve descripción del riesgo y terminar con la consecuencia. Ejemplo:
"La falta en reclutar, capacitar y retener personal competente, inhibe la habilidad de la institución para ejecutar, manejar y supervisar actividades clases de la entidad"

Mantener la definición breve.
Una descripción breve, de alto nivel, permite a los participantes pensar ampliamente acerca de la variedad de causas y efectos de los riesgos. La discusión y análisis durante el proceso de evaluación, facilita el identificar si es necesario una definición más específica.

Desarrollar la forma de documentación adaptada a la entidad, usando un lenguaje común.
El universo de riesgos debe proveer un lenguaje común. El adaptar riesgos genéricos incorporando el vocabulario de la institución ayuda a que la forma de lenguaje usado sea mejor comprendido.

Para la elaboración de este artículo se utilizo información del blog: www.nahunfrett.blogspot.com

Ética y probidad:

Directriz 20(*) Prohíbe a los funcionarios públicos dar recomendaciones a personas privadas

Artículo 1°—Los funcionarios públicos no deben, haciendo uso de los recursos del Estado o la influencia que surja de un cargo público, emitir recomendaciones a personas físicas o jurídicas. Esta prohibición incluye las recomendaciones para otorgamiento de préstamos o sobregiros a empresas o particulares en instituciones financieras.

Se exceptúan de esta disposición las recomendaciones de tipo académico y humanitario, y las recomendaciones laborales que se refieren a relaciones de servicio anteriores a la ostentación del cargo público. En estos casos debe hacerse mención expresa del destinatario, del propósito y de la condición en que se emite la recomendación. En ningún caso se podrá utilizar papelería u otros recursos del Estado.

Artículo 2°—las instituciones públicas deben realizar una evaluación de las disposiciones administrativas de rango inferior a la ley que establecen la obligación de presentar referencias personales como requisito para la prestación de servicios en el sector público o el reconocimiento de determinados derechos. Las disposiciones reglamentarias o circulares dictadas en ese sentido deben señalar que las recomendaciones deben ser veraces y corresponder a relaciones laborales, comerciales, académicas o personales, ciertas y susceptibles de ser comprobadas.

Artículo 3°—La inobservancia de las anteriores disposiciones acarreará las sanciones administrativas que correspondan.

(*) Fecha de vigencia desde el 04/04/1997 Publicada en Gaceta No. 65 del 04/04/1997

Estimados compañeros les recordamos que en la dirección: https://pani.go.cr/auditoria-interna/boletin-audinforma/

Se encuentran disponibles para consulta las ediciones anteriores de boletín Audinforma que han sido generados por nuestra instancia.

Agradecemos mucho los aportes sugerencias y recomendaciones para la mejora del producto:

Consultas o sugerencias, escribanos: audinforma@pani.go.cr