AudInforma

- a su servicio

Febrero 2023 No. 2

En esta segunda edición queremos compartir con todos los funcionarios de la institución información relevante respecto a.

1. Ciberseguridad y teletrabajo: Como protegernos de las ciber amenazas durante el teletrabajo

2. Seguridad de la información y protección de datos en el teletrabajo

3. Servicio de Asesoría: referente a los ajustes incorporados en las Normas Técnicas sobre Presupuestos Públicos relacionados con la gestión institucional de Fideicomisos

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.

CIBERSEGURIDAD Y TELETRABAJO: COMO PROTEGERNOS DE LAS CIBER AMENAZAS DURANTE EL TELEGRABAJO

Para disponer de un entorno de teletrabajo seguro, y protegernos de ciber amenazas es importante considerar una serie de aspectos entre los que están:

1. El cumplimiento de las políticas, lineamientos y direccionamientos que en materia de ciber seguridad y teletrabajo son dispuestos desde los diferentes instancias institucionales relacionadas con dicha materia. El cumplimiento de las políticas de teletrabajo y ciberseguridad promueven ambientes de trabajo virtual más seguros y contribuyen a la protección de la información institucional.

2. La capacitación y aprendizaje en temas de ciber seguridad. La capacitación en temas de ciberseguridad es un aspecto muy necesario para evitar posibles riesgos y proporciona conocimientos para desarrollar habilidades que nos permitan laborar de manera virtual en una forma más segura. Esta capacitación puede ser desarrollada a través de charlas, cursos virtuales, actividades dinámicas, videos, presentaciones.

3. La implementación de buenas prácticas durante el teletrabajo que contribuyan a fortalecer las políticas institucionales y la protección de los sistemas de información y los datos contenidos en los mismos.

Continua en la siguiente página

SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS EN EL TELETRABAJO

El trabajo desde casa implica el acceso a programas, plataformas o sistemas institucionales de manera remota. Por esto es importante contemplar medidas de seguridad de la información y protección de datos.

Algunas medidas de seguridad importantes a considerar son:

- ✓ Usar siempre las herramientas de conexión proporcionadas por la institución (VPN, plataformas de videoconferencias, etc.).
- ✓ Cuando se use WIFI, hay que recordar que este debe ser seguro y estar protegido con contraseña.
- ✓ El equipo desde el que se trabaja debe disponer de antivirus y tener actualizado el sistema operativo, con las actualizaciones de seguridad necesarias.
- ✓ Se debe evitar dejar sesiones abiertas al entorno institucional, accesibles por terceros, ya que se podría comprometer o poner en riesgo información confidencial.
- ✓ No se deben anotar en libretas o notas, usuarios y contraseñas institucionales que puedan ser accedidos o usados por terceros.
- ✓ El acceso en remoto que se nos proporciona la institución no debe ser usado para acceder desde equipos o entornos que no sean autorizados.

Además para evitar caer en trampas que puedan poner en riesgo la información y datos institucionales, es importante considerar:

Ser prudente con la apertura de correos electrónicos: si no estás esperando el correo, no tiene nada que ver contigo, está redactado con faltas o es de un remitente desconocido, sé prudente y no abras sus adjuntos ni pulses en sus enlaces.

Acceder a las páginas oficiales directamente para obtener información fiable y legítima: no pulses en enlaces de WhatsApp, SMS, e-mails, etc. que pueden redirigir a falsas webs

Mucho cuidado con descargar apps no oficiales: puedes comprometer tus dispositivos y la información contenida en ellos.

Evitar el uso de memorias extraíbles no autorizadas: Las memorias flash (USB) no autorizadas por el equipo de seguridad TI pueden incrementar exponencialmente el riesgo de sufrir una falla de seguridad en el dispositivo siendo uno de los mecanismos más frecuentes para la introducción de un malware.

En el presente artículo se utilizó información contenida en: Guía de buenas prácticas para el trabajo telemático durante el confinamiento por Covid-19

SERVICIO DE ASESORÍA: referente a los ajustes incorporados en las Normas Técnicas sobre Presupuestos Públicos relacionados con la gestión institucional de Fideicomisos

¿CÚAL ES EL ORIGEN?

La auditoria interna en colaboración con la Contraloría General de la República, se encuentra realizado actividades de seguimiento a las gestiones y decisiones relacionadas con la ejecución del Contrato de Fideicomiso PANI BNCR durante su periodo de vigencia, así como lo relativo al finiquito contractual.

Como parte del trabajo, se conoció de los ajustes efectuados por el ente contralor a la Normativa Técnica sobre Presupuestos Públicos N-1-2012- DC-DFOE, esto a partir de la entrada en vigencia de la Ley General de Contratación Pública No. 9986, relacionados con Fideicomisos, los cuales se encuentran incorporados en la Resolución R-DC-117-2022 del Despacho Contralor

¿POR QUÉ ES IMPORTANTE?

El servicio de asesoría tiene como propósito brindar insumos a la Administración del PANI, que contribuyan a implementar controles presupuestarios que integren el presupuesto institucional y los recursos públicos complementarios y vinculados a su gestión que se manejan mediante fideicomisos, a fin de mejorar la trazabilidad de la información y fortalecer la transparencia y asegurar una rendición de cuentas de alta calidad, de manera uniforme, íntegra y objetiva.

Las Normas Técnicas sobre Presupuestos Públicos actualizadas y con la totalidad de ajustes indicados, pueden ser consultados y descargados, en la siguiente dirección:

https://www.cgr.go.cr/03-documentos/normativa/prespub.html

BIENVENIDA COMPAÑERA

Por este medio le damos la bienvenida a la compañera Karla Torres Sánchez, quien a partir del 15 de Febrero se incorpora a la Auditoria Interna, desde ya le deseamos muchos éxitos, bienvenida al equipo de trabajo.

Consultas o sugerencias, escribanos: audinforma@pani.go.cr
Además consulte las ediciones anteriores del boletín en la web:
https://pani.go.cr/auditoria-interna/boletin-audinforma/