

Revelador Institucional # 05 - Boletín de Control Interno

Comunicaciones Internas ANI <comunicacionesinternasani@ani.gov.co>

Jue 30/07/2020 11:18 AM

**Boletín 05****Y CON TRABAJO EN CASA ¿CÓMO ESTÁ LA ANI EN MATERIA DE CIBERSEGURIDAD?**

La Presidencia de la República, contemplando la situación actual del País debido a la Pandemia del COVID-19, dispuso en la Directiva Presidencial 02 de 2020, atender la contingencia con el uso de las Tecnologías de la Información y las Telecomunicaciones – TIC.

[1] En consecuencia, **la Entidad para garantizar el cumplimiento de estos lineamientos implementó como medida preventiva de carácter temporal y extraordinario el trabajo en casa, trabajo virtual en casa o trabajo remoto**, que no es más que “un mecanismo excepcional mediante el cual los servidores públicos podrán realizar sus actividades desde un lugar diferente al de su trabajo habitual, de manera remota y colaborativa haciendo uso de las Tecnologías de la Información y las Comunicaciones existentes” diferente a la definición de teletrabajo.



Teniendo en cuenta lo anterior y el uso de las tecnologías de la información (desde equipos de escritorio, portátiles tabletas y smartphones hasta servidores), la Entidad se puede ver afectada en una amplia gama de incidentes potencialmente desastrosos, como por ejemplo, los ciberdelincuentes que están aprovechando la situación actual para lanzar ataques enfocados en el trabajo en casa. Para ello utilizan métodos muy variados, desde acceso a sistemas con contraseñas poco seguras u obtenidas por otros medios (Ingeniería Social), hasta capturar el tráfico de datos que pasan por redes Wi-Fi poco seguras.

Además, la actual preocupación por el Coronavirus está generando muchas campañas o promociones atrayentes y una vez capturada la atención, mediante técnicas de phishing, logran que los usuarios bajen la guardia atraídos por la curiosidad y capturan sus datos de identificación y bancaria. Lo anterior deja en evidencia la identificación de nuevos riesgos asociados a este tipo de situaciones, que las organizaciones no siempre contemplan dentro de su planeación[2].

Teniendo en cuenta estos posibles riesgos, durante el pasado mes de mayo, **la Oficina de Control Interno realizó una auditoría asociada al cumplimiento de la Entidad en materia de ciberseguridad por el trabajo en casa a causa del COVID-19; al respecto se evidenciaron, a través de la gestión realizada por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones, las siguientes fortalezas en esta materia:**

1. **Se han planeado, implementado y cubierto los protocolos de seguridad necesarios para garantizar el blindaje de la red de la Entidad**, el monitoreo permanente y el cubrimiento de las necesidades de la Entidad en materia de cifrado, autenticación y fortaleza en la política de contraseñas.
2. **Se han planeado, implementado y monitoreado las conexiones remotas** para garantizar el buen funcionamiento y el soporte permanente.

3. **Se han planeado, implementado y realizado las copias de seguridad y probado la restauración de estos respaldos** lo cual garantiza la recuperación de información clave ante eventuales interrupciones del servicio.
4. **Se han identificado concienzudamente y gestionado los riesgos de ciberseguridad y como consecuencia de la situación actual se ha revisado la identificación de nuevos riesgos**, lo que ha permitido el refinamiento en el tratamiento de los riesgos existentes. Lo anterior se ha manifestado en la no materialización de riesgos y en la efectiva gestión de la infraestructura de TI incluida la seguridad y disponibilidad de la información.
5. **Se han planeado, implementado y monitoreado permanentemente los recursos y se evidencia eficiencia y eficacia en la distribución de los recursos.**

Es importante tener presente que mejorar el conocimiento y la preparación de los colaboradores de la Entidad sobre los peligros a los que se encuentra expuesto por la implementación de trabajo en casa, fortalecerá la seguridad de la Entidad.

Los invitamos a no bajar la guardia y a estar siempre alerta con situaciones que pueden poner en riesgo la información de la Entidad y la personal. De igual manera, estar siempre a la vanguardia en el conocimiento y gestión de las tendencias y nuevos riesgos, debido a que la tecnología es dinámica y cambia con frecuencia, para ello es importante identificar riesgos nuevos que contribuyan a la mitigación de situaciones no deseadas y formular controles que las prevengan y/o detecten.

¹ https://encrypted-tbn0.gstatic.com/images?q=tbn%3AAND9GcQDOfgc7ZQN6Bu_aHgM55w7U1aOy5udHd_JoA&usqp=CAU

² Auditoría al HW, SW, SI y Ciberseguridad: https://www.ani.gov.co/sites/default/files/auditoria_a_hw_sw_si_ciberseguridad.pdf



Comunicaciones Internas ANI
Servicios
Oficina de Comunicaciones
Presidencia
PBX: 571 - 484 8860 Ext:
Calle 24 A Nro. 59 - 42 Edificio T4, Piso 2
Bogotá D.C. - Colombia - www.ani.gov.co



"Resolución 0666 del 24 de abril de 2020 expedida por el Ministerio de Salud y Protección Social Principales medidas de bioseguridad:

- Lávese las manos frecuentemente.
- Use el tapabocas cubriendo nariz y boca.
- Practique el distanciamiento físico.
- Lo invitamos a descargar y reportar diariamente su condición de salud en la Aplicación CoronApp-Colombia o en Alissta si está afiliado a la ARL POSITIVA.



Por favor piense en el medio ambiente antes de Imprimir este correo

La información contenida en este correo electrónico es propiedad de la Agencia Nacional de Infraestructura.: es confidencial y para uso exclusivo de el (los) destinatario(s) / En la Agencia Nacional de Infraestructura respetamos y garantizamos que los datos personales suministrados por usted, a través de nuestros canales de comunicación, estén protegidos y no se divulgarán sin su consentimiento. Cumplimos con nuestra política de Confidencialidad y Protección de Datos. Si quiere conocerla lo invitamos a consultarla en: <https://www.ani.gov.co/contenido/politicas-tic>. Si ha recibido este mensaje por error, por favor notifíquese inmediatamente al remitente: no copie, imprima, distribuya ni difunda su contenido. Las opiniones, conclusiones e informaciones que no estén relacionadas directamente con el negocio de la Agencia Nacional de Infraestructura. deben entenderse como personales y no están avaladas por la compañía.