COMUNICADO N°004-2022-PCM/SGTD/CNSD

DIRIGIDO A: ENTIDADES PÚBLICAS
Oficiales de Seguridad y Confianza Digital
Jefes de las Oficinas de Tecnologías de la Información y Comunicaciones

En el marco del Decreto Legislativo N°1412, el Decreto de Urgencia N°006-2020 y sus normas reglamentarias, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, ejerce la rectoría en materia de gobierno, confianza y transformación digital en el país, y viene liderando el despliegue de tecnologías digitales en favor de garantizar el acceso inclusivo, seguro y de calidad al entorno digital en todas las regiones del país para consolidar la ciudadanía digital como lo establece la Política General de Gobierno 2021-2026.

En virtud de ello, y en cumplimiento del lineamiento 8.1.5 de la Política General de Gobierno que *"Consolidar las acciones de seguridad y confianza digital para la protección de la ciudadanía frente a los riesgos y amenazas en el entorno digital"*, la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros viene impulsando las coordinaciones con las entidades y organizaciones integrantes del Sistema Nacional de Transformación Digital a fin de fortalecer la confianza digital en el país.

El Centro Nacional de Seguridad Digital gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital y se encuentra a cargo de la Secretaría de Gobierno y Transformación Digital.

El Centro Nacional de Seguridad Digital es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza y es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos y constituye el mecanismo de intercambio de información y articulación de acciones con los responsables de los ámbitos del Marco de Seguridad Digital del Estado Peruano

En este contexto, se hace necesario comunicar que se ha identificado un listado de dominios ransomware, dominios CONTI, IP CONTI en los cuales se viene distribuyendo el malware (listado que se proporciona en archivo adjunto); por lo tanto, las entidades públicas deben tomar las previsiones del caso para implementar, en el menor tiempo posible, las siguientes recomendaciones:

- Incluir todos los indicadores de compromiso (anexo a este documento) a sus firewalls o sistemas de detección de intrusos como fines preventivos en sus infraestructuras tecnológicas.
- Incorporar la lista de dominios (anexo a este documento) en las listas negras de los diferentes activos a nivel de software y hardware del sector.
- Los datos e información de los sistemas de información deben ser transmitidos y almacenados de forma cifrada.
- Se debe implementar un sistema de detección y prevención de intrusos en diferentes zonas de la red
- Se debe implementar un firewall de aplicaciones WAF.
- Se debe implementar un firewall de base de datos.
- Se debe implementar el monitoreo permanente de los servicios ofrecidos para garantizar su disponibilidad, así como también la trazabilidad de las operaciones
- Implementar sistemas de protección y seguridad DNS. Asimismo, tener actualizado los procesos de licenciamiento de los diferentes activos a nivel de software y hardware.

- Cambiar de contraseñas a todos los usuarios de todas las plataformas.
- Implementar de forma obligatoria la autenticación multifactor en los diferentes sistemas de información.
- Realizar una revisión completa de los usuarios creados para cada uno de los sistemas informáticos y de comunicación.
- Verificar su política de copias de seguridad (backup) y realizar las pruebas de restauración.
- Realizar una revisión de la salida de internet de todos los servidores de la institución.
- Mantener actualizadas las firmas de la solución de antivirus.

Es importante indicar que el Centro Nacional de Seguridad Digital emite diariamente alertas integradas de seguridad digital que son puestas a disposición de la ciudadanía, empresas y entidades públicas: https://www.gob.pe/institucion/pcm/colecciones/791-alerta-integrada-de-seguridad-digital-del-cnsd

Asimismo, se han publicado políticas de seguridad digital y de seguridad de la información para avanzar en el despliegue de acciones para prevenir ciberataques: https://www.gob.pe/institucion/pcm/colecciones/4951-formatos-de-politicas-de-seguridad-de-la-informacion

Finalmente es importante recordar que, conforme a lo establecido en el Artículo 9. Del Decreto de Urgencia N°007-2020: Obligaciones del Proveedor de servicios digitales:

9.1 Las entidades de la administración pública, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos, deben:

a. **Notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.**
b. Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.
c. Gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información.
d. Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de riesgo del mismo y de acuerdo a la normatividad vigente en materia de protección de datos personales.
e. Mantener una infraestructura segura, escalable e interoperable.
f. Toda actividad crítica debe estar soportada en una infraestructura segura, disponible, escalable e interoperable.

Todo incidente de seguridad digital puede reportarse en a través del correo: incidentes@cnsd.gob.pe y/o la plataforma https://facilita.gob.pe/t/1025

El equipo del Centro Nacional de Seguridad Digital estará alerta a las situaciones que puedan presentarse.

CENTRO NACIONAL DE SEGURIDAD DIGITAL
Secretaría de Gobierno y Transformación Digital
PRESIDENCIA DEL CONSEJO DE MINISTROS