RESOLUCIÓN ADMINISTRATIVA
N° 000189-2021-CE-PJ

Artículo Primero.- Implementan el Equipo de Respuestas ante Incidentes de Seguridad Digital del Poder Judicial (CSIRT-PJ).

Artículo Segundo.- Disponen que el Equipo de Respuestas ante Incidentes de Seguridad Digital del Poder Judicial, estará presidido por el Gerente de Informática de la Gerencia General del Poder Judicial, con experiencia en Ciberseguridad y normatividad digital, quien gestionará el equipo, tomando en consideración la siguiente conformación de roles:

a. Gerente de Informática del Poder Judicial, quien lo presidirá.

b. Gestor de Incidentes.

c. Responsable del Soporte de primer nivel de incidentes.

d. Responsable del Soporte de segundo nivel de incidentes.

Para la conformación del equipo, el Gerente de Informática podrá designar al personal de la Gerencia de Informática que cumpla los roles indicados.

Artículo Tercero.- El Equipo de Respuestas ante Incidentes de Seguridad Digital del Poder Judicial, tiene las siguientes funciones:

a. Realizar la verificación de los eventos en ciberseguridad en redes y telecomunicaciones reportados en el Poder Judicial.

b. Determinar si un evento de ciberseguridad en redes y telecomunicaciones reportado se convierte en incidente, y comunicarlo al Centro Nacional de Seguridad Nacional.

c. Activar los mecanismos de colaboración para la coordinación y gestión de incidentes entre entidades.

d. Coordinar acciones con el Centro Nacional de Seguridad Nacional y otras entidades especializadas en ciberseguridad, para mantener o restaurar la continuidad de los servicios informáticos ante los incidentes en redes y telecomunicaciones.

e. Prevenir futuros incidentes en redes y telecomunicaciones.

f. Implementar un sistema automatizado para la gestión de incidentes.

g. Monitorear la implementación del plan de continuidad del negocio en todas las Cortes Superiores a nivel nacional

h. Proveer asistencia técnica, asesorías y apoyo a la comunidad, entidades públicas y privadas, para proteger las plataformas tecnológicas ante amenazas y/o incidentes informáticos y prevenir futuros ataques, dificultades o eventos que afecten la confidencialidad e integridad de los datos.

i. Brindar asistencia y atención con el fin de ayudar a tomar medidas para proteger y asegurar las plataformas tecnológicas, prever futuros ataques, dificultades o eventos que afecten la confidencialidad e integridad de la información.

j. Brindar la asesoría a las entidades públicas y privadas para la rápida recuperación ante incidentes.

k. Establecer los procedimientos legales de atención de incidentes de ciberseguridad.

l. Establecer alianzas estrategias con organismos nacionales e internacionales, entidades públicas y privadas, para afianzar los mecanismos de ayuda mutua en materia de ciberseguridad.

m. Generar estrategias para suministrar un sistema de alertas tempranas, anuncios y comunicados que permitan prevenir los riesgos asociados al uso de las tecnologías de la información y comunicaciones.

n. Promover en las organizaciones públicas y privadas la creación e integración de esquemas de atención de incidentes de seguridad.

o. Realizar las acciones conducentes a la reducción del impacto de los incidentes en redes y telecomunicaciones.

p. Efectuar servicios proactivos de ciberseguridad establecidos y creados a través de estándares y buenas prácticas para mejorar la seguridad, generando recomendaciones, comentarios y sensibilizaciones con base en las lecciones aprendidas.

q. Efectuar análisis de vulnerabilidad para evidenciar las debilidades de ciberseguridad que pueden tener los portales web o los sistemas informáticos.

r. Auditar la infraestructura de tecnología de la información y comunicaciones, para detectar no conformidades y emitir las respectivas recomendaciones.

s. Coordinar con las entidades correspondientes si los incidentes que se presentan son acompañados de conductas delictivas, con el fin de realizar la recolección de evidencias para esclarecer los hechos e investigaciones que se puedan generar.

t. Difundir información sobre vulnerabilidades, técnicas de ataques o virus informáticos entre otras, que son detectados por las firmas de antivirus o por software especializado, con el fin de alertar a las plataformas tecnológicas.

u. Realizar el monitoreo de la infraestructura tecnología policial y de igual forma a las páginas web de los dominios del Poder Judicial identificando alertas sobre ataques que se generen y tomar las acciones conjuntas necesarias para contrarrestarlos.

v. Formular y difundir el boletín informativo que contiene información útil, para mejorar la seguridad de la información.

w. Efectuar vigilancia tecnológica.

x. Efectuar actividades de sensibilización en ciberseguridad, mediante charlas, conferencias, boletines, videos y eventos, para generar conciencia en los usuarios sobre los riesgos que puedan vulnerar la seguridad.

y. Desarrollar el análisis de riesgos de la infraestructura de tecnología de la información y comunicaciones.

z. Coordinar con las Oficinas de Tecnología de la Información y Comunicaciones de las Cortes Superiores a nivel nacional, con el fin de tratar en un espacio académico, los temas necesarios para fortalecer las capacidades técnicas y operativas que deben tener, para prevenir y contrarrestar las amenazas que atente la ciberseguridad

Artículo Cuarto.- Las dependencias y los órganos del Poder Judicial comprometidos, accionarán en las áreas de su competencia, para la debida implementación del Equipo de Respuestas ante Incidentes de Seguridad Digital del Poder Judicial.