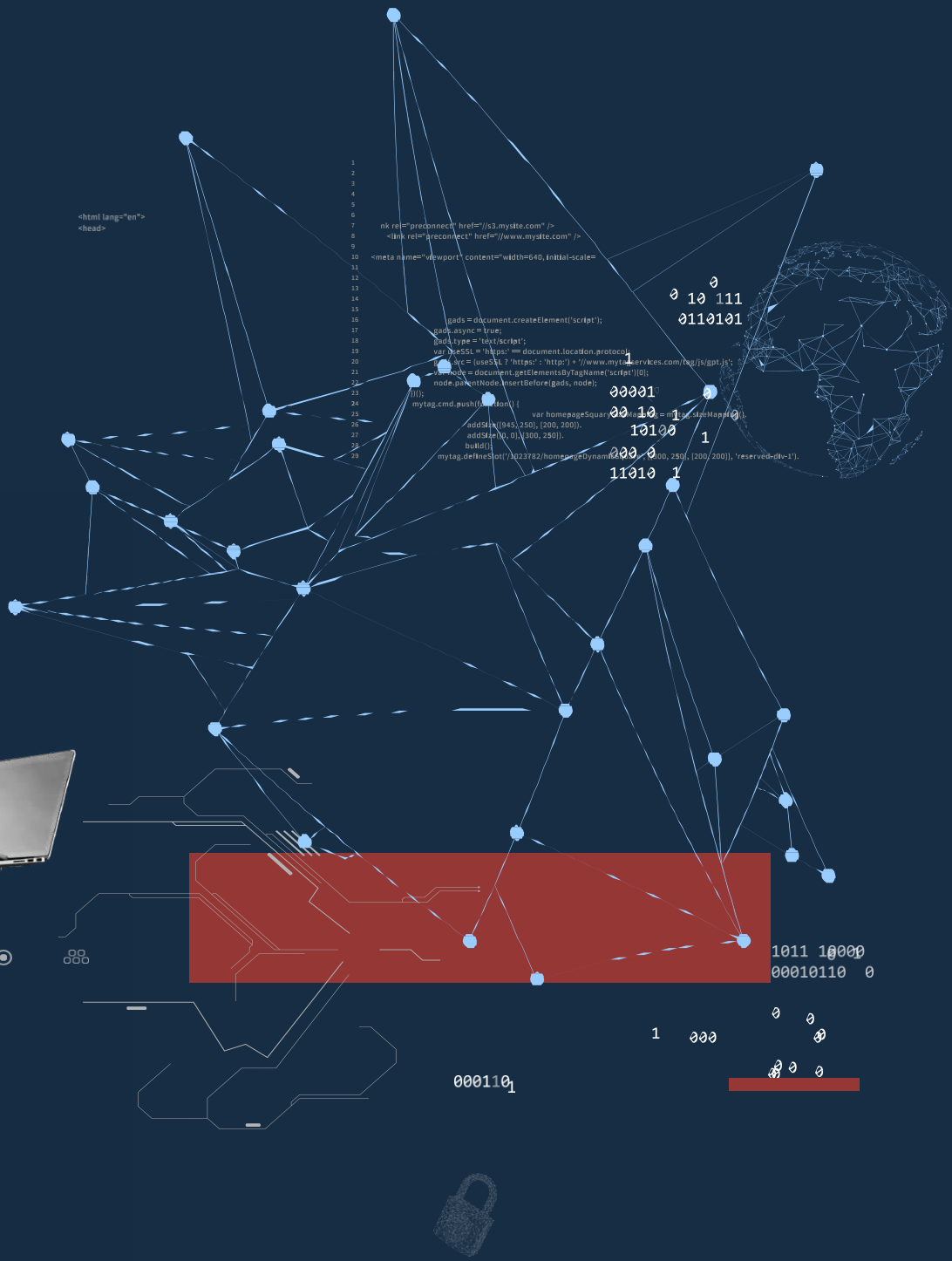
Ministerio del Interior y Seguridad Pública

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

SI ENFRENTA UN CIBERATAQUE, SU EQUIPO DEBE TENER LAS SIGUIENTES CAPACIDADES



I.- ACTUAR CON RAPIDEZ

Cada minuto cuenta cuando un malware ha ingresado en nuestros sistemas y está encriptando nuestros datos. Cada miembro de la organización debe tener claro su rol, para no perder tiempo, actuar coordinadamente, y realizar una respuesta eficiente y eficaz al ataque. Hay que actuar rápido, pero en lo posible en base a playbooks escritos y probados, pues un error en la primera respuesta puede costarle muy caro a la institución.

II.- ENTENDER LA SITUACIÓN Y GUIAR A LA ORGANIZACIÓN

Los responsables de ciberseguridad deben comprender el ataque y transmitir información a la organización de modo comprensible y con instrucciones para actuar en la práctica. La primera evaluación debe aportar indicadores preliminares que permitan ponderar la criticidad e impacto del incidente para poner al tanto al jefe de servicio si el incidente pone en riesgo la continuidad operacional de los servicios institucionales o afecta gravemente su reputación.

III.- PROCEDER EFICAZ Y COORDINADAMENTE

Los responsables de ciberseguridad deben manejar, conocer y poder coordinar con los equipos de operaciones la actuación de las diferentes plataformas de control de incidencias dentro de su infraestructura TI, con el objetivo de contener, aislar y mitigar el riesgo lo antes posible. Gracias a que cada uno conoce su rol, el líder de ciberseguridad puede coordinar a los miembros del equipo para que apliquen los planes de la política de ciberseguridad de la organización. En la cadena de coordinación del incidente es clave el cumplimiento normativo de notificación obligatoria al CSIRT de Gobierno y requerir su ayuda si el incidente no se está logrando contener o aislar.

IV.- PROCESAR GRANDES VOLÚMENES DE DATOS

El equipo de ciberseguridad debe ser capaz de procesar un mayor volumen de datos del habitual, para entender los vectores de ataque y puntos calientes del malware, con el objetivo de responder al ciberataque y mantener la disponibilidad de sus servicios. Contemplar necesidad de obtener capacidad en la nube y apoyo de unidades análisis automatizados basados en IA, para alivianar y acelerar el procesamiento masivo de información que provendrá de múltiples dispositivos.

V.- JUDICIALIZAR

Tenga presente que un incidente puede llegar a clasificarse posteriormente como un delito informático, razón por la cual dentro del protocolo de respuesta a incidentes deben estar incluidas las consideraciones para no afectar la evidencia o pruebas digitales que servirán posteriormente para judicializar el delito. Pruebas digitales bien preservadas podrán usarse ante un juicio y tendrán el mismo valor probatorio que una evidencia física, y ayudarán a la fiscalía y policías a encontrar a los responsables

¿Estás preparado?

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1510

@CSIRTGOB

https://www.linkedin.com/company/csirt-gob

https://www.instagram.com/csirtgobcl

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile