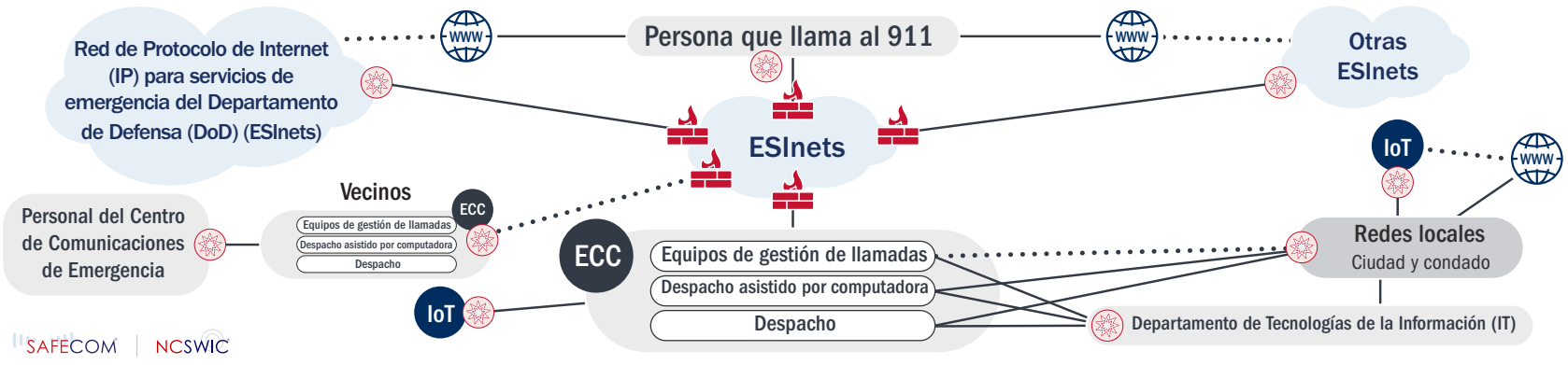
DOS COSAS QUE TODO CENTRO DE 911 DEBERÍA HACER PARA MEJORAR LA CIBERSEGURIDAD

SUPERFICIES DE CIBERATAQUE AL 911



https://www.cisa.gov/safecom/transition-next-generation-911 | Diagrama basado en las superficies de cibera taque al NG911 del CSRIC.

La ruta más directa del país para recibir asistencia de emergencia, el sistema 911, requiere comunicaciones estables, seguras y sólidas. Delincuentes sofisticados y Estados nación explotan las vulnerabilidades cibernéticas como amenaza para la prestación de servicios esenciales. La integración de nuevas tecnologías, como la multimedia, amplía los vectores de amenazas y la mayor interconexión de sistemas plantea amenazas en una superficie de ataque más amplia.

La ciberseguridad es una responsabilidad compartida. Todas las organizaciones desempeñan un papel, y a algunas se les exige que cumplan con estándares, como el Estándar para Comunicaciones de Servicios de Emergencia (NFPA 1225) de la Asociación Nacional de Protección contra Incendios (NFPA), para mejorar la posición en materia de ciberseguridad. SAFECOM, el Consejo Nacional de Coordinadores de Interoperabilidad Estatal (NCSWIC, por sus siglas en inglés), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés), el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) y otros socios tienen recursos útiles. La ciberseguridad se ha convertido en una parte integral de la función de la misión y las operaciones de los sistemas heredados y del 911 de próxima generación (NG911, por sus siglas en inglés). El trabajo conjunto con otros actores de la comunidad, el gobierno, la industria y el mundo académico para establecer estándares, políticas, procedimientos y directrices de interoperabilidad y aplicación consistentes para la implementación del NG911 es crucial.

EVALUACIÓN DE RIESGOS CIBERNÉTICOS

Las evaluaciones de riesgos de ciberseguridad (cibernéticos) ayudan a los centros de comunicaciones de emergencia (ECC, por sus siglas en inglés) y a los puntos de respuesta de seguridad pública (PSAP, por sus siglas en inglés) a comprender las vulnerabilidades y amenazas a sus operaciones (por ejemplo, misión, funciones, imagen, reputación), activos organizacionales e individuos. Una evaluación de riesgos cibernéticos puede ayudar a un centro de comunicaciones de emergencia (ECC) o punto de respuesta de seguridad pública (PSAP) a determinar los siguientes pasos para proteger sus sistemas y redes de agentes maliciosos y fallos en la infraestructura.

A continuación, se presentan recursos que pueden ayudar a los centros de comunicaciones de emergencia (ECC) y a los puntos de respuesta de seguridad pública (PSAP) a realizar evaluaciones cibernéticas:

- SAFECOM, *Guía para empezar a realizar una* evaluación de riesgos cibernéticos
- CISA, *Kit de inicio de Cyber Essentials: los conceptos básicos para crear una culturade preparación cibernética*
- CISA, *Kit de herramientas de comunicaciones de seguridad pública y resiliencia cibernética*
- CISA, *Hoja informativa sobre recursos de resiliencia cibernética para la seguridad pública*
- NIST, *Marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés)*

PLANES DE RESPUESTA A CIBERINCIDENTES Y VULNERABILIDADES

Los planes de respuesta a incidentes cibernéticos y de respuesta a vulnerabilidades brindan orientación para identificar y mitigar incidentes que puedan afectar los sistemas y las operaciones de los centros de comunicaciones de emergencia (ECC) y los puntos de respuesta de seguridad pública (PSAP), así como medidas de respuesta y recuperación ante estos. Es fundamental garantizar que todos los usuarios y dispositivos, la infraestructura de red y las conexiones, los datos, las aplicaciones de datos y los servicios se evalúen por completo para evitar interrupciones. Es necesario contar con un plan de respuesta a incidentes para minimizar las brechas en los servicios, evitar la pérdida de datos y servicios, y garantizar la continuidad de las operaciones. Los planes de respuesta a vulnerabilidades abordan los pasos a seguir con respecto a las amenazas y vulnerabilidades de ciberseguridad identificadas. Es esencial trabajar de manera coordinada con las partes interesadas y los proveedores de servicios para desarrollar acuerdos mutuos conjuntos sobre la continuidad de las operaciones durante una crisis relacionada con ciberataques. La recuperación de datos, las pruebas y la capacitación son componentes fundamentales de los planes de respuesta, y la coordinación con todas las partes interesadas y los socios puede ayudar a que la transición sea fluida.

A continuación, se presentan recursos que pueden ayudar a los centros de comunicaciones de emergencia (ECC) y a los puntos de respuesta de seguridad pública (PSAP) a desarrollar planes de respuesta a incidentes cibernéticos:

- CISA, *Manuales de respuesta a incidentes de ciberseguridad y vulnerabilidades del Gobierno federal*
- CISA, *Elementos esenciales: su respuesta ante una crisis*
- CISA, *Alertas cibernéticas*
- CISA, *Respuesta a incidentes cibernéticos*

¿CÓMO PUEDE PARTICIPAR NUESTRO ECC O PSAP?

Realizar evaluaciones periódicas de riesgos cibernéticos y, en función de los resultados:

- Desarrollar planes de respuesta a incidentes y vulnerabilidades, planes de recuperación y planes de continuidad de operaciones (COOP, por sus siglas en inglés) para ayudar en la respuesta a incidentes de ciberseguridad.
- Ejecutar planes que se puedan validar, perfeccionar y actualizar.
- Incorporar las lecciones aprendidas en los procesos y las estrategias de planificación de la recuperación.
- Capacitar al personal de respuesta en las últimas prácticas operativas, de seguridad y de resiliencia y planes de continuidad de operaciones (COOP) y mantener una formación continua a medida que se disponga de nuevas tecnologías y métodos.
- Mantener la coordinación y comunicación con otros socios, proveedores y partes interesadas, como el coordinador de interoperabilidad estatal (SWIC, por sus siglas en inglés).
- Coordinar con los proveedores de servicios al desarrollar y actualizar planes de respuesta cibernética.
- Los centros de comunicaciones de emergencia (ECC) y los puntos de respuesta de seguridad pública (PSAP) deberían considerar implementar capacidades de detección y mitigación de amenazas cibernéticas y utilizar recursos como las capacidades de la Agencia de Seguridad Cibernética y de la Infraestructura (CISA) y los centros de fusión. Estos centros estatales y locales pueden proporcionar monitoreo del sistema, identificación de amenazas e intercambio de inteligencia, lo que permite a los centros de comunicaciones de emergencia (ECC) y puntos de respuesta de seguridad pública (PSAP) mantener una posición cibernética proactiva.
- Familiarizarse con los casos prácticos de respuesta a incidentes cibernéticos y comprender y priorizar las amenazas que afectan la misión de la agencia.
- Considerar implementar el servicio de 911 de próxima generación (NG911), que mantiene una autenticación avanzada y capacidades de seguridad mejoradas.

RECURSOS ADICIONALES SOBRE CIBERSEGURIDAD

Para obtener más información sobre esta y otras iniciativas de ciberseguridad, envíe un correo electrónico a ng911wg@cisa.dhs.gov o visite cisa.gov/safecom/next-generation-911 y cisa.gov.