DESARROLLO DE LOS TRABAJADORES

IDENTIFICACIÓN DE NECESIDADES

- Identifique sus necesidades de carga de trabajo.
  - Evalúe la complejidad de sus operaciones y la velocidad con la que las acciones deben ejecutarse.
  - Analice las necesidades de capacidad de reacción y si las tecnologías avanzadas pueden ayudar a reducir la superficie de ataque.
- Identifique las necesidades de su plantilla.
  - Tenga en cuenta la competencia, flexibilidad y agilidad del personal de ciberseguridad de su organización.
  - Identifique las estructuras ideales para la presentación de informes y destaque dónde es preferible la multifuncionalidad.
- Defina los conocimientos, habilidades, destrezas y competencias necesarios de la plantilla de ciberseguridad en función de las funciones empresariales que apoyan.
- Identifique las lagunas críticas en el personal de ciberseguridad existente en su organización.
  - Utilice los instrumentos existentes, como el marco NICE, para orientar las evaluaciones internas de las funciones y responsabilidades.

AVANCE DE LA FORMACIÓN Y EL DESARROLLO INTERNOS

- Desarrolle planes profesionales que resalten las vías de progreso de su personal de ciberseguridad.
- Identifique las rutas dentro de su organización para la formación y el traslado del personal a funciones de ciberseguridad.
  - Considere posibles puntos de entrada no tradicionales en la ciberseguridad en función del interés y la capacidad.
  - Amplíe los programas de capacitación y formación e incentive las transiciones dentro de su organización.
- Promueva la formación interna y el aprendizaje independiente.
  - Brinde oportunidades para la educación continua y la certificación de habilidades.
  - Realice un seguimiento de los datos sobre la permanencia de la plantilla.
  - Evalúe los datos de permanencia periódicamente para identificar si los programas de formación y desarrollo están satisfaciendo las necesidades de los empleados.

MEJORA DE LA CONTRATACIÓN EXTERNA

- Refuerce los anuncios de empleo escribiendo descripciones de trabajo claras y coherentes internamente.
  - Utilice las herramientas existentes, como el marco NICE, para destacar los conjuntos de aptitudes pertinentes.
- Recopile datos sobre la contratación a través del proceso de solicitud, y capture los tipos de candidatos y su experiencia laboral previa.
  - Sistematice la recogida de datos y compártalos en toda la empresa para evitar la formación de silos y favorecer la búsqueda y el desarrollo de talento.
  - Evalúe periódicamente los datos de contratación para identificar las lagunas en la difusión.
- Confíe en múltiples indicadores para evaluar el potencial de los candidatos.
  - Considere la posibilidad de aplicar evaluaciones sistematizadas de la contratación.
  - Evalúe los títulos, certificaciones y experiencias laborales pertinentes.
  - Evite basarse en una métrica específica (p. ej., un máster en ingeniería) al tomar decisiones de contratación.

Enfoques fundamentales

Considere los siguientes enfoques estratégicos al desarrollar una plantilla de ciberseguridad.

1. **Amplíe la línea de suministro** para obtener talentos nuevos.
   - ¿Tiene relaciones con universidades y escuelas técnicas?
   - ¿Ofrece prácticas o formación en ciberseguridad?
2. **Identifique y combine la oferta existente** con las oportunidades de talento.
   - ¿Su departamento de recursos humanos está trasladando eficazmente los perfiles requeridos a las descripciones de los puestos de trabajo anunciados?
3. **Vuelva a formar** al **personal existente** para que forme parte de la plantilla cibernética.
   - ¿Su organización está aprovechando el talento existente trasladando recursos a su plantilla cibernética?
4. **Reduzca la demanda** de su plantilla cibernética a través de la **innovación tecnológica**.
   - ¿Tiene acuerdos con proveedores de servicios externos para crear capacidad de reacción durante períodos críticos?
5. **Mejore la permanencia** de la plantilla actual.
   - ¿Su organización está invirtiendo en miembros del equipo con talento?
   - ¿Su organización permite a las personas interesadas explorar oportunidades profesionales en el campo de la ciberseguridad?

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE
INTERNATIONAL MONETARY FUND
THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA INDEPENDENT COMMUNITY BANKERS of AMERICA®