COMPETENCIA • ETAPA

RESILIENCIA DE LA INFORMACIÓN Y CIBERSEGURIDAD

PREPARACIÓN

1. Identificar los eventos que pueden generar una afectación de la seguridad de la información y la ciberseguridad (ataques de denegación de servicio, secuestro de información, ataques cibernéticos, entre otros).

2. Definir y designar los roles y responsabilidades necesarios para recuperar la operación del negocio (comité de seguridad de la información y ciberseguridad, líder de recuperación y protección de TI).

3. Definir estrategias para la respuesta ante la afectación de la seguridad de la información y la ciberseguridad.

4. Implementar y documentar controles para la protección de la s eguridad de la información y la ciberseguridad.

5. Definir planes para la respuesta ante la afectación de la seguridad de la información y la ciberseguridad.

6. Mantener contacto con los grupos de interés de los que se requiere apoyo para la respuesta ante la afectación de la seguridad de la información y la ciberseguridad.

RESPUESTA

7. Activar estructura organizacional para responder a la afectación de la seguridad de la información y la ciberseguridad.

8. Monitorear el cumplimiento de los protocolos de Bioseguridad implementados para la operación del negocio cuando se requiera apoyo en sitio de personal.

9. Monitorear el desarrollo de la situación, así como gestionar las necesidades que se deriven del evento que se está materializando.

10. Mantener contacto con los grupos de interés que correspondan al tipo de evento que se está materializando (CSIR-PONAL, proveedores TIC, entre otros).

RECUPERACIÓN

11. Verificar que el evento se encuentre controlado.

12. Definir las nuevas condiciones de operación y políticas de los servicios TIC.

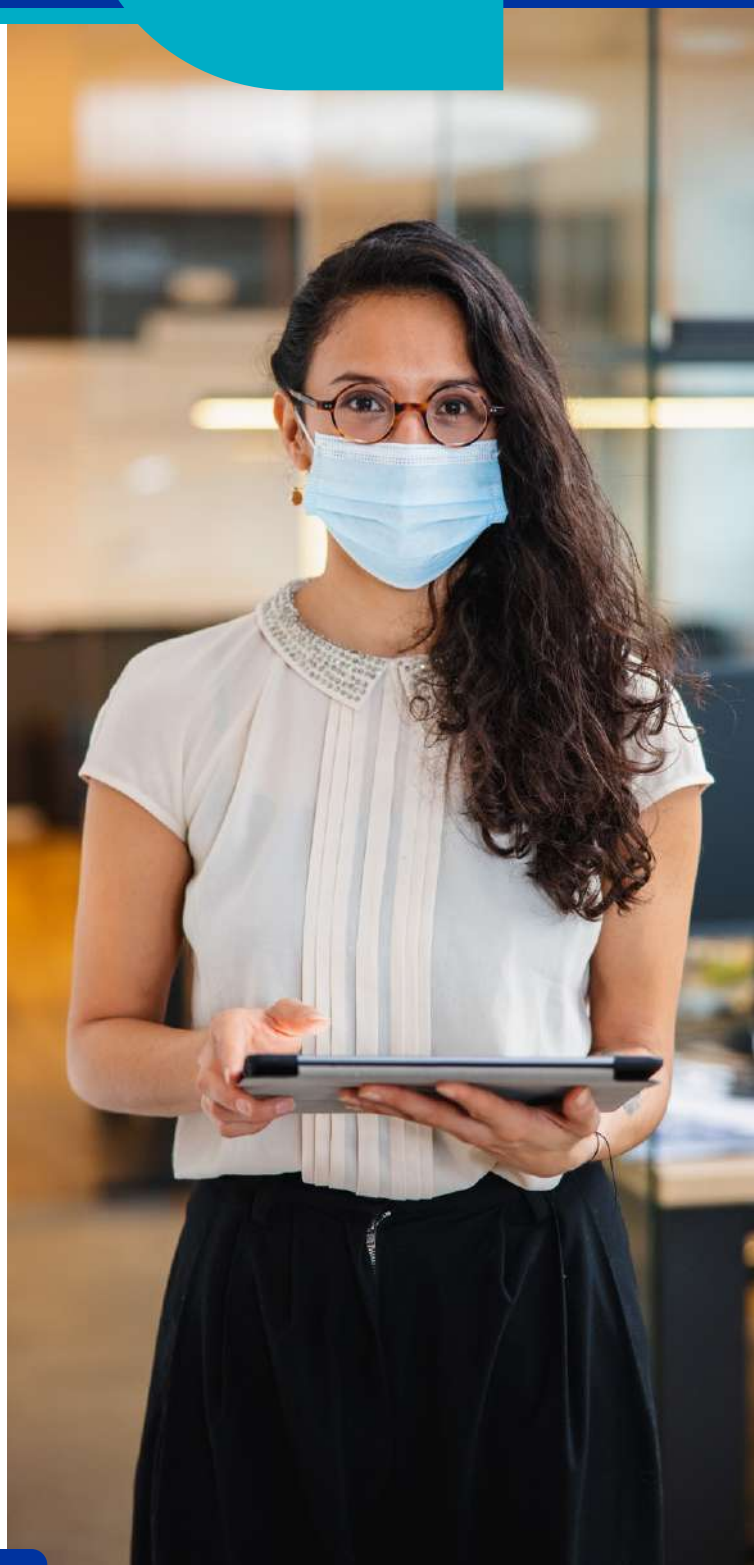
13. Definir, desplegar y comunicar el plan de reanudación de los servicios TIC.

14. Comunicar oportunamente a las condiciones de reanudación de los servicios TIC a los integrantes de los grupos de interés que corresponda (empleados, contratistas, proveedores, clientes, entre otros).

REANUDACIÓN

15 Verificar la operación y protección de los servicios TIC.

16 Monitorear el entorno, validando que las condiciones de seguridad y ciberseguridad se mantengan.



¡JUNTOS NOS ASEGURAMOS

DE AVANZAR!