



CONTINUIDAD DE LA RED

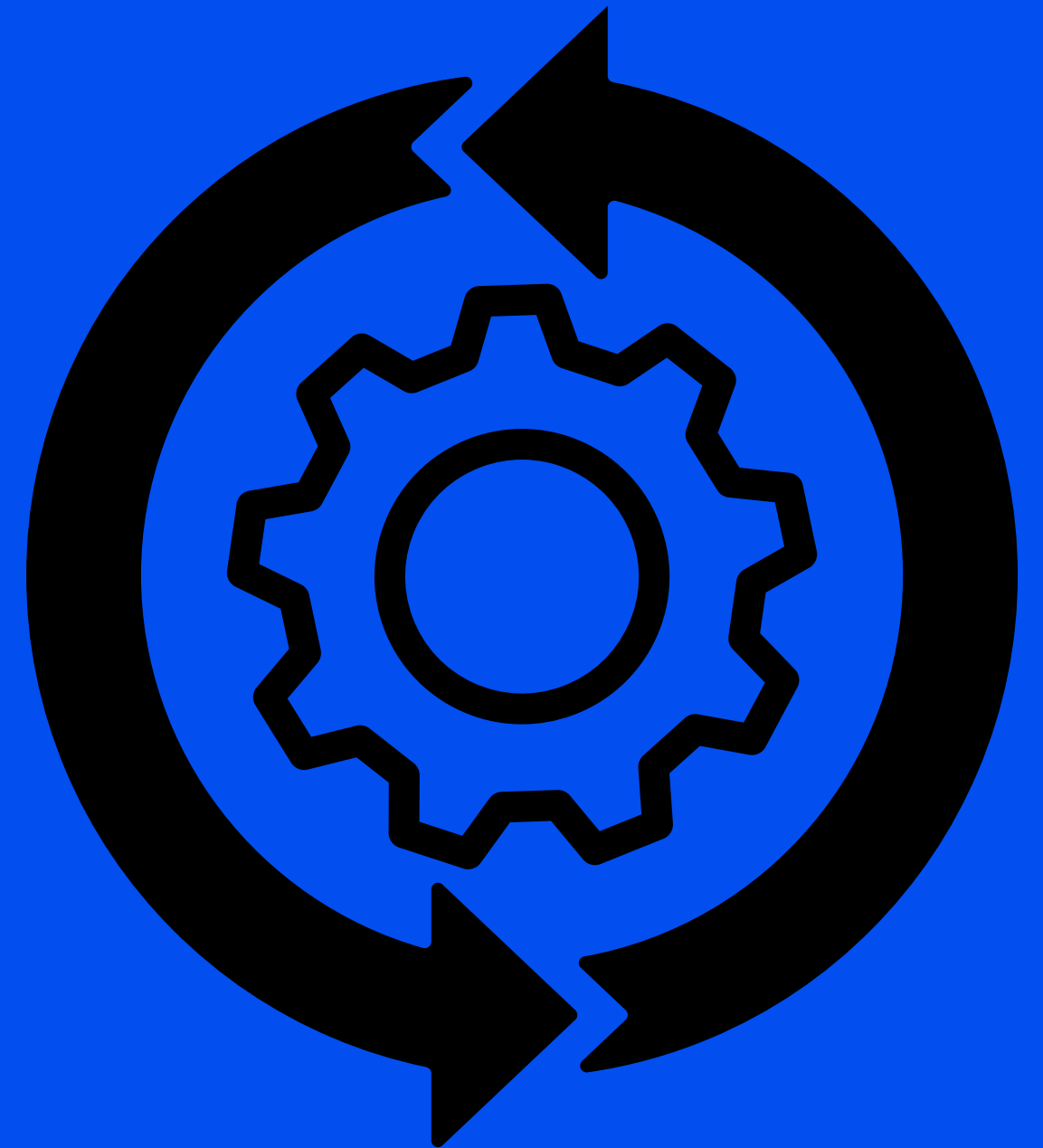
IBARRA JIMÉNEZ JESÚS
LAZCANO AGUILAR GILMAR ALDAIR
RAMÍREZ GONZÁLEZ KARLA
SOTO BLANCAS MARCO ANTONIO
VENANCIO REA JESE ZURIEL

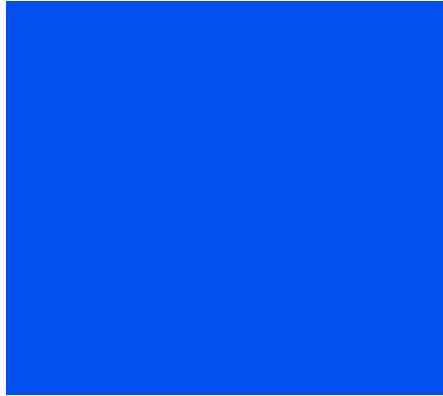
3.3.3



CONCEPTO

LA CONTINUIDAD DE LA RED ES LA CAPACIDAD DE UNA ORGANIZACIÓN PARA MANTENER LA DISPONIBILIDAD DE SUS SERVICIOS DE RED, INCLUSO FRENTE A INTERRUPCIONES, DESASTRES, O FALLAS TÉCNICAS. ESTE CONCEPTO ES ESENCIAL PARA PREVENIR IMPACTOS NEGATIVOS EN LA PRODUCTIVIDAD, EL FLUJO DE INFORMACIÓN Y LA COMUNICACIÓN CON CLIENTES Y PROVEEDORES, ASEGURANDO QUE LOS PROCESOS CRÍTICOS SIGAN FUNCIONANDO.





IMPORTANCIA DE LA CONTINUIDAD DE LA RED

- **ROL CENTRAL DE LA RED:** LA RED CONECTA APLICACIONES, BASES DE DATOS, SERVICIOS EN LA NUBE Y EMPLEADOS. LA PÉRDIDA DE CONECTIVIDAD AFECTA EL RENDIMIENTO GENERAL Y LA OPERATIVIDAD DE LA ORGANIZACIÓN.
- **IMPACTO FINANCIERO Y REPUTACIONAL:** LAS INTERRUPCIONES DE LA RED PUEDEN RESULTAR EN PÉRDIDA DE INGRESOS, DAÑO A LA REPUTACIÓN Y DISMINUCIÓN DE LA CONFIANZA DE LOS CLIENTES. EJEMPLOS: EMPRESAS QUE DEPENDEN DEL COMERCIO ELECTRÓNICO O SERVICIOS EN LÍNEA PUEDEN VER PÉRDIDAS SIGNIFICATIVAS EN CUESTIÓN DE MINUTOS DE DESCONEXIÓN.



PRINCIPALES AMENAZAS



FALLOS DE HARDWARE Y SOFTWARE:

PROBLEMAS CON ROUTERS, SWITCHES, FIREWALLS, O CONFIGURACIONES INCORRECTAS PUEDEN AFECTAR EL TRÁFICO DE DATOS.



CIBERATAQUES:

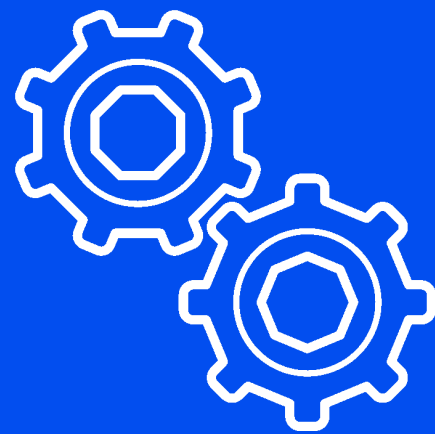
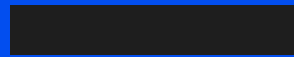
LOS ATAQUES DE DENEGACIÓN DE SERVICIO (DDOS) SATURAN LA RED, IMPIDIENDO EL ACCESO LEGÍTIMO. OTROS ATAQUES PUEDEN COMPROMETER LA SEGURIDAD Y LA CONTINUIDAD DE LOS DATOS.



DESASTRES NATURALES:

INUNDACIONES, INCENDIOS, TERREMOTOS O TORMENTAS PUEDEN DAÑAR FÍSICAMENTE LA INFRAESTRUCTURA DE RED, INCLUYENDO CABLES Y SERVIDORES.

PLAN DE CONTINUIDAD DE LA RED (PCN)

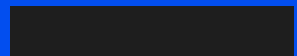


DEFINICIÓN.

UN PCN ES UN CONJUNTO DE POLÍTICAS, PROCEDIMIENTOS Y ACCIONES PLANIFICADAS PARA ASEGURAR QUE LA RED CONTINÚE FUNCIONANDO O SEA RECUPERABLE EN CASO DE INTERRUPCIÓN.



COMPONENTES PRINCIPALES



- IDENTIFICACIÓN DE RIESGOS: DETECCIÓN DE AMENAZAS Y VULNERABILIDADES ESPECÍFICAS DE LA RED.
- PROCEDIMIENTOS DE RECUPERACIÓN: PASOS DETALLADOS PARA RESTAURAR SERVICIOS DE RED TRAS UNA FALLA.
- ROLES Y RESPONSABILIDADES: ASIGNACIÓN DE TAREAS ESPECÍFICAS A PERSONAL CAPACITADO PARA EJECUTAR EL PLAN EN CASO DE EMERGENCIA.
- PRUEBAS Y REVISIÓN PERIÓDICA: VALIDACIÓN Y ACTUALIZACIÓN DEL PCN PARA ASEGURAR SU EFECTIVIDAD.



EVALUACIÓN DE RIESGOS

- **ANÁLISIS DE RIESGOS:** INVOLUCRA IDENTIFICAR AMENAZAS ESPECÍFICAS QUE PUEDEN AFECTAR LA RED, COMO CIBERATAQUES, CORTES DE ENERGÍA, Y FALLOS DE HARDWARE. ESTE ANÁLISIS INCLUYE TANTO LA PROBABILIDAD DE OCURRENCIA COMO EL POSIBLE IMPACTO.

- **IDENTIFICACIÓN Y PRIORIZACIÓN:** CLASIFICACIÓN DE RIESGOS POR SU NIVEL DE SEVERIDAD Y FRECUENCIA.
EJEMPLO: LOS FALLOS DE HARDWARE CRÍTICOS, COMO EN LOS SERVIDORES PRINCIPALES, PUEDEN TENER PRIORIDAD DEBIDO A SU IMPACTO EN TODA LA RED.
- **MAPEO DE VULNERABILIDADES:** DETECCIÓN DE PUNTOS DÉBILES EN LA RED Y SISTEMAS CRÍTICOS, COMO CONEXIONES SIN REDUNDANCIA.

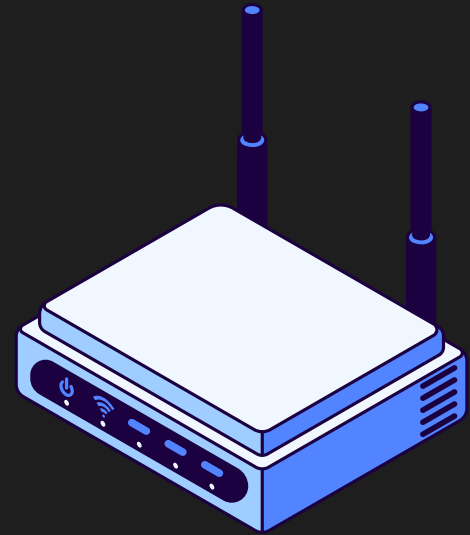
ESTRATEGIAS DE RESPALDO

BACKUPS DE RED: CONFIGURAR COPIAS DE SEGURIDAD DE CONFIGURACIONES DE RED, BASES DE DATOS Y ARCHIVOS CRÍTICOS DE FORMA PROGRAMADA. ESTO PERMITE RESTAURAR CONFIGURACIONES Y SERVICIOS TRAS UN FALLO.

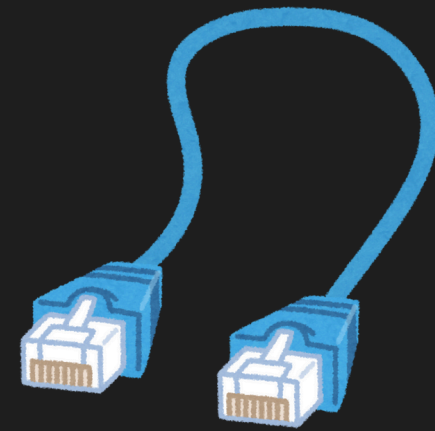
DISASTER RECOVERY PLAN (DRP): ESTRATEGIAS PARA LA RECUPERACIÓN DE OPERACIONES TRAS EVENTOS DE INTERRUPCIÓN. UN DRP INCLUYE MANTENER UNA RÉPLICA DE LA RED EN UN CENTRO DE DATOS ALTERNATIVO, USO DE TECNOLOGÍAS DE VIRTUALIZACIÓN Y RESPALDO EN LA NUBE PARA RESTAURAR LOS SERVICIOS.

TESTING DE RECUPERACIÓN: REALIZAR PRUEBAS PERIÓDICAS PARA ASEGURAR QUE LOS BACKUPS Y EL PLAN DE RECUPERACIÓN FUNCIONEN CORRECTAMENTE Y SEAN ACTUALES.

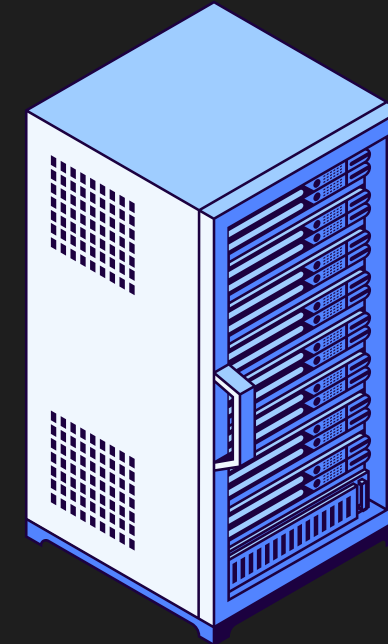
REDUNDANCIA DE LA INFRAESTRUCTURA



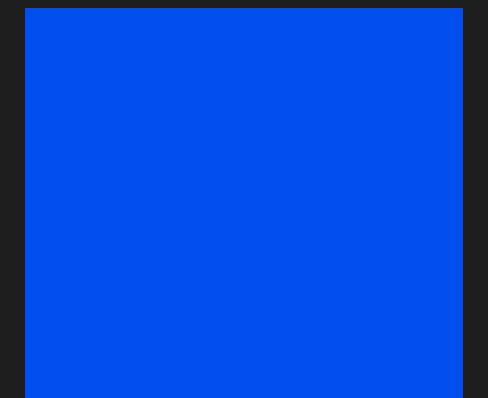
REDUNDANCIA DE HARDWARE:
IMPLEMENTAR SISTEMAS
DUPLICADOS PARA
ROUTERS, SWITCHES, Y
SERVIDORES
ESENCIALES. ESTOS
SISTEMAS ENTRAN EN
FUNCIONAMIENTO
AUTOMÁTICAMENTE SI
LOS PRINCIPALES
FALLAN.



REDUNDANCIA DE RUTAS
Y CONEXIONES:
CONFIGURACIÓN DE
RUTAS ALTERNATIVAS
PARA QUE EL TRÁFICO DE
RED TENGA OPCIONES EN
CASO DE FALLOS EN LA
CONEXIÓN PRINCIPAL.
POR EJEMPLO, TENER
MÚLTIPLES ENLACES A
PROVEEDORES DE
INTERNET.



BALANCEO DE CARGA:
USO DE TECNOLOGÍAS
DE BALANCEO PARA
DISTRIBUIR EL TRÁFICO
DE RED ENTRE VARIOS
SERVIDORES,
REDUCIENDO LA CARGA
EN UN SOLO EQUIPO Y
MEJORANDO LA
DISPONIBILIDAD.



MONITOREO Y DETECCIÓN DE PROBLEMAS

HERRAMIENTAS DE MONITOREO EN TIEMPO REAL: USO DE SOLUCIONES COMO NAGIOS, ZABBIX, O SOLARWINDS PARA SUPERVISAR LA RED CONTINUAMENTE Y ALERTAR DE POSIBLES PROBLEMAS ANTES DE QUE CAUSEN INTERRUPCIONES.

ALERTAS Y RESPUESTAS AUTOMÁTICAS: CONFIGURACIÓN DE ALERTAS QUE SE ACTIVEN CON CONDICIONES PREDEFINIDAS, COMO UN USO INUSUAL DE ANCHO DE BANDA, PARA TOMAR ACCIÓN RÁPIDA Y REDUCIR EL TIEMPO DE INACTIVIDAD.


ANÁLISIS DE RENDIMIENTO Y CAPACIDAD: MONITOREO CONTINUO DEL DESEMPEÑO DE LA RED PARA PREVER PROBLEMAS POR SATURACIÓN O CONGESTIÓN.

ENTRENAMIENTO Y SIMULACIÓN




CAPACITACIÓN DEL EQUIPO:

FORMACIÓN DE LOS EQUIPOS DE TI Y DE RED EN LOS PROCEDIMIENTOS Y HERRAMIENTAS DEL PCN. ESTO ASEGURA QUE EL PERSONAL CLAVE PUEDA RESPONDER EFICAZMENTE A CUALQUIER INCIDENTE.



SIMULACROS Y EJERCICIOS DE PRUEBA:

REALIZACIÓN DE SIMULACROS DE INTERRUPCIÓN PARA PROBAR EL TIEMPO DE RESPUESTA Y EFECTIVIDAD DEL PCN, ASÍ COMO LA COORDINACIÓN DEL EQUIPO DURANTE UN INCIDENTE.



EVALUACIÓN DE RESULTADOS Y MEJORAS:

TRAS CADA SIMULACRO, REALIZAR UNA REVISIÓN DETALLADA DE LOS RESULTADOS Y AJUSTAR EL PLAN SEGÚN LOS APRENDIZAJES OBTENIDOS.

MEJORA CONTINUA

EVALUACIÓN Y ACTUALIZACIÓN:
REVISAR Y ACTUALIZAR
PERIÓDICAMENTE EL PCN PARA
ADAPTARSE A CAMBIOS
TECNOLÓGICOS, NUEVOS
RIESGOS Y LECCIONES
APRENDIDAS DE INCIDENTES
PASADOS.

LECCIONES APRENDIDAS: ANALIZAR
CADA INTERRUPCIÓN Y EVALUAR LA
EFECTIVIDAD DE LAS RESPUESTAS
PARA MEJORAR LA RESILIENCIA DE LA
RED Y REDUCIR EL IMPACTO DE
FUTUROS PROBLEMAS.

INNOVACIÓN Y
ADAPTACIÓN:
INTEGRAR NUEVAS
TECNOLOGÍAS Y
PRÁCTICAS, COMO
INTELIGENCIA
ARTIFICIAL PARA
DETECCIÓN
PROACTIVA DE
AMENAZAS, A FIN
DE FORTALECER LA
CONTINUIDAD DE
LA RED.