UNIVERSIDAD RAFAEL LANDÍVAR
FACULTAD DE INGENIERÍA
ESTRATEGIAS DE CONTINUIDAD DE NEGOCIO

Caso: " Ataque de Ransomware en el Centro Médico Springhill "

RAFAEL ANDRÉS ALVAREZ MAZARIEGOS 1018419
XIMENA STEPHANIA ELIZARDI GOBERN 1101720
EDDIE ALEJANDRO GIRÓN CARRANZA 1307419
JULIO ANTHONY ENGELS RUIZ COTO 1284719
CÉSAR ADRIAN SILVA PÉREZ 1184519

GUATEMALA DE LA ASUNCIÓN, OCTUBRE DE 2024
CAMPUS CENTRAL “SAN FRANCISCO DE BORJA, S. J” DE LA CIUDAD DE GUATEMALA

Link de la presentación:
https://www.canva.com/design/DAGVfH0Zkks/xwh6CayxbCpVklNcKCczfw/edit?utm_content=DAGVfH0Zkks&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

1. Evaluación de la Respuesta al Incidente

- ¿Cómo actuó Springhill Medical Center en las primeras horas? Evaluar si las decisiones iniciales contribuyeron a controlar o escalar el problema.
    - Según su comunicado del 16 de julio, cerraron su red inmediatamente para contener el incidente y proteger los datos tras el ataque de ransomware. Notificaron a las autoridades y contrataron expertos forenses externos para investigar la situación. A pesar del ataque, el personal continuó brindando atención a los pacientes por medios extraoficiales de comunicación, utilizando maquinaria vieja y sin mayor comunicación sobre lo sucedido con el ataque.
    - Las acciones tomadas, si bien lograron contribuir a que el ataque no siguiera propagándose en su red, llegó a ser muy perjudicial operativamente debido al nivel de dependencia del hospital en su tecnología y que no se tenían instaurados procesos de respaldo.
- ¿Qué medidas de contención se aplicaron para detener la propagación del ransomware? Comparar con prácticas recomendadas en recuperación ante desastres.
    - Como se mencionó anteriormente las acciones para contener el ataque fueron la desconexión de red, informar a autoridades sobre el incidente y la implementación de procesos manuales, para evitar usar el sistema.
    - Según TD SYNNEX en su LAC BLOG, las 5 mejores prácticas recomendadas para recuperación de desastres incluyen contar con un comité de recuperación de desastres, poseer copias de seguridad o Backups como servicios (BaaS) junto con prácticas de recuperación automatizadas en la nube o contratar un servicio de recuperación de desastres. Tomando en cuenta estos 5 factores y comparándolos con las acciones realizadas por SMC, podemos llegar a la conclusión que se implementaron algunas medidas de contención inmediatas, como la desconexión de la red, pero estas acciones resultaron insuficientes para mantener la continuidad operativa y la

calidad en la atención médica. La falta de una planificación de recuperación de desastres estructurada, respaldada por prácticas recomendadas como un comité de recuperación, BaaS, y DRaaS, limitó severamente la capacidad de SMC para manejar el ataque de ransomware de forma efectiva y segura para los pacientes.

- Examinar los tiempos de restauración de sistemas y los pasos que tomaron para retomar el servicio.
    - Springhill Medical Center (SMC) experimentó una restauración de sistemas prolongada, que se extendió por tres semanas después del ataque de ransomware. Finalmente, se logró restablecer los servicios esenciales, aunque tomó más tiempo para que el hospital volviera a estar completamente operativo. No se especifica los pasos específicos que se tomaron para retomar el servicio. Sin embargo, en estándares promedio, según Acronis Cyber Protect, SMC se recupero bajo la norma de 22 días.

2. Evaluación de la Comunicación

- ¿Cómo se manejó la información entre los equipos? ¿Hubo una comunicación clara y rápida para apoyar la respuesta?
    - Fue de manera indirecta, a través de post its inicialmente indicando que el sistema estaba abajo, tampoco se informó formalmente que problemas tenía en si el hospital que dio espacio a rumores. Según el documento, la única comunicación clara que se tuvo fue la de no mencionar nada a los medios.
- Analizar la claridad y transparencia de la comunicación del hospital hacia los empleados, médicos, pacientes, familiares y stakeholders. ¿Se manejó de manera que se preservara la confianza pública?
    - Empleados y Médicos: La falta de información precisa generó confusión y rumores, aumentando el estrés y la incertidumbre entre el personal.
    - Pacientes y Familiares: No se informó adecuadamente sobre el impacto del ciberataque en la atención médica, limitando su capacidad para tomar decisiones informadas.
    - Declaraciones Públicas: Los comunicados fueron vagos y tardíos, sin detalles claros sobre el ataque, lo que generó dudas en la comunidad y stakeholders.
    - Confianza Pública: La falta de transparencia afectó la confianza en el hospital, debilitando la percepción de seguridad y fiabilidad.

- ¿De qué manera la comunicación (o falta de ella) influyó en la percepción del incidente y en la confianza de los pacientes?
    - Al no ser claros con el impacto o alcance del ataque, o el tiempo en el que lanzaban los comunicados, hacia parecer que el ataque no era lo que fue y que todo estaba trabajando normalmente, cuando no era así. Haciendo creer a los pacientes que el hospital seguía siendo una buena opción para sus tratamientos, ocasionando accidentes o muertes evitables como se presentó en este caso. Afectando la imagen del hospital permanentemente.

3. Recomendaciones desde el Punto de Vista de Recuperación ante Desastres

Fortalecimiento del Plan de Respuesta: ¿Qué recomendaciones específicas haría para mejorar la respuesta ante ataques similares en el futuro? Ejemplos: segmentación de redes, backups fuera de línea, y recuperación de datos.

1. Implementación de Segmentación de Redes

- Descripción: Dividir la red del hospital en segmentos aislados para limitar la propagación de amenazas y proteger sistemas críticos.
- Pasos a Seguir:
    - Realizar una auditoría completa de la infraestructura de red existente.
    - Diseñar una nueva arquitectura de red segmentada.
    - Implementar firewalls internos y sistemas de detección y prevención de intrusiones (IDS/IPS).
    - Configurar políticas de acceso y comunicación entre segmentos.

Costos Estimados:

Concepto	Costo Estimado
Auditoría de Red	$ 20,000
Equipamiento de Red (Switches, Firewalls, IDS/IPS)	$ 80,000
Software de Gestión de Red	$ 2,000 (anuales)
Mano de Obra (Ingenieros de Redes)	$ 40,000
Total Aproximado	$ 142,000

2. Implementación de Autenticación Multifactor (MFA)

- Descripción: La MFA agrega una capa adicional de seguridad al requerir múltiples formas de verificación antes de conceder acceso a sistemas y datos.

- Pasos a Seguir:
    - Evaluar y seleccionar una solución MFA compatible con los sistemas existentes.
    - Integrar MFA en todos los sistemas críticos y aplicaciones.
    - Capacitar al personal en el uso de MFA.

Costos Estimados:

Concepto	Costo Estimado
Licencias de MFA (1,000 usuarios)	$ 30,000 (anuales)
Implementación y Configuración	$ 15,000
Soporte	$ 5,000 (anuales)
Total Aproximado	$ 50,000

3. Implementación de Backups Fuera de Línea

- Descripción: Realizar copias de seguridad regulares y almacenarlas en ubicaciones fuera de línea para prevenir su encriptación durante un ataque de ransomware.
- Pasos a Seguir:
    - Adquirir soluciones de almacenamiento seguras (cintas magnéticas, almacenamiento en frío).
    - Establecer políticas de backup frecuentes (diarias, semanales).
    - Automatizar el proceso de backup y verificar su integridad.
    - Almacenar copias de seguridad en ubicaciones físicas separadas.

Costos Estimados:

Concepto	Costo Estimado
Dispositivos de Almacenamiento (Cintas, Unidades)	$ 25,000
Software de Backup y Recuperación	$ 20,000 (anuales)
Instalación y Configuración	$ 10,000
Capacitación del Personal	$ 5,000 (anuales)
Total Aproximado	$ 60,000

4. Contratación de Servicios de Centro de Operaciones de Seguridad (SOC) 24/7

- Descripción: Un SOC proporciona monitoreo continuo, detección de amenazas y respuesta a incidentes en tiempo real.
    - Pasos a Seguir:

- Evaluar proveedores de servicios SOC gestionados (MSSP).
- Establecer acuerdos de nivel de servicio (SLA) claros.
- Integrar los sistemas del hospital con el SOC.

Costos Estimados:

Concepto	Costo Estimado
Servicios SOC Gestionados	$ 150,000 (anuales)
Integración Inicial	$ 20,000
Total Aproximado	$ 170,000

Resumen de Costos para el Fortalecimiento del Plan de Respuesta:

Concepto	Costo Estimado
Licencias de MFA (1,000 usuarios)	$ 30,000 (anuales)
Soporte	$ 5,000 (anuales)
Servicios SOC Gestionados	$ 150,000 (anuales)
Software de Gestión de Red	$ 2,000 (anuales)
Software de Backup y Recuperación	$ 20,000 (anuales)
Capacitación del Personal	$ 5,000 (anuales)
Total Aproximado	$ 212,000.00

Concepto	Costo Estimado
Auditoría de Red	$ 20,000
Equipamiento de Red (Switches, Firewalls, IDS/IPS)	$ 80,000
Mano de Obra (Ingenieros de Redes)	$ 40,000
Implementación y Configuración	$ 15,000
Dispositivos de Almacenamiento (Cintas, Unidades)	$ 25,000
Instalación y Configuración	$ 10,000
Integración Inicial	$ 20,000
Total Aproximado	$ 210,000.00

$ 422,000.00

Mejora de Procedimientos de Comunicación: Recomendaciones para una comunicación efectiva, tanto interna como externa, que ayude a la organización a responder rápidamente y a preservar su reputación.

1. Implementación de Herramientas de Comunicación de Emergencia

- Descripción: Utilizar sistemas dedicados para alertar y comunicar información crítica al personal durante incidentes.
  - Pasos a Seguir:
  - Seleccionar una plataforma de notificación de emergencia (por ejemplo, Everbridge, AlertMedia).
  - Configurar listas de distribución y protocolos de alerta.
  - Capacitar al personal en el uso y recepción de alertas.

Costos Estimados:

Concepto	Costo Estimado
Licencias de la Plataforma	$ 38,000 (anuales)
Configuración Inicial	$ 5,000
Capacitación del Personal	$ 5,000 (anuales)
Total Aproximado	$ 48,000

2. Formación en Comunicación de Crisis para el Equipo Directivo

- Descripción: Capacitar a los líderes y portavoces de la organización en habilidades de comunicación efectiva durante situaciones de crisis.
    - Pasos a Seguir:
    - Identificar Portavoces Clave: Seleccionar a las personas que serán la voz oficial durante una crisis.
    - Organizar Talleres y Entrenamientos: Realizar sesiones de formación con expertos en comunicación.
    - Practicar con Simulaciones: Llevar a cabo simulacros de ruedas de prensa y entrevistas.

Costos Estimados:

Concepto	Costo Estimado
Sesiones de Capacitación (5 días)	$ 15,000
Materiales y Recursos Didácticos	$ 2,000
Total Aproximado	$ 17,000

3. Implementación de Boletines Internos y Externos Durante Incidentes

- Descripción: Distribuir regularmente boletines informativos que proporcionen actualizaciones y detalles sobre la situación.
    - Pasos a Seguir:
    - Establecer un Calendario de Publicación: Definir la frecuencia y horarios de los boletines.
    - Crear Contenido Relevante: Incluir información útil para diferentes audiencias.
    - Distribución Multicanal: Enviar boletines por correo electrónico, intranet, sitios web y redes sociales.

Costos Estimados:

Concepto	Costo Estimado
Software de Email Marketing	$ 180 (anuales)
Diseño y Redacción de Contenido	$ 12,000
Total Aproximado	$ 12,180

Resumen de Costos para la Mejora de Procedimientos de Comunicación:

Concepto	Costo Estimado
Licencias de la Plataforma	$ 38,000 (anuales)
Capacitación del Personal	$ 5,000 (anuales)
Software de Email Marketing	$ 180 (anuales)
Total Aproximado	$ 43,180.00

$ 77,180.00

Concepto	Costo Estimado
Configuración Inicial	$ 5,000
Sesiones de Capacitación (5 días)	$ 15,000
Materiales y Recursos Didácticos	$ 2,000
Diseño y Redacción de Contenido	$ 12,000
Total Aproximado	$ 34,000.00

Preparación Continua

Propuesta de un plan que permita estar preparados para afrontar un incidente similar.

1. **Análisis de Riesgos**

   Identificar y evaluar los riesgos relacionados con ciberataques, especialmente ataques de ransomware y determinar las vulnerabilidades.

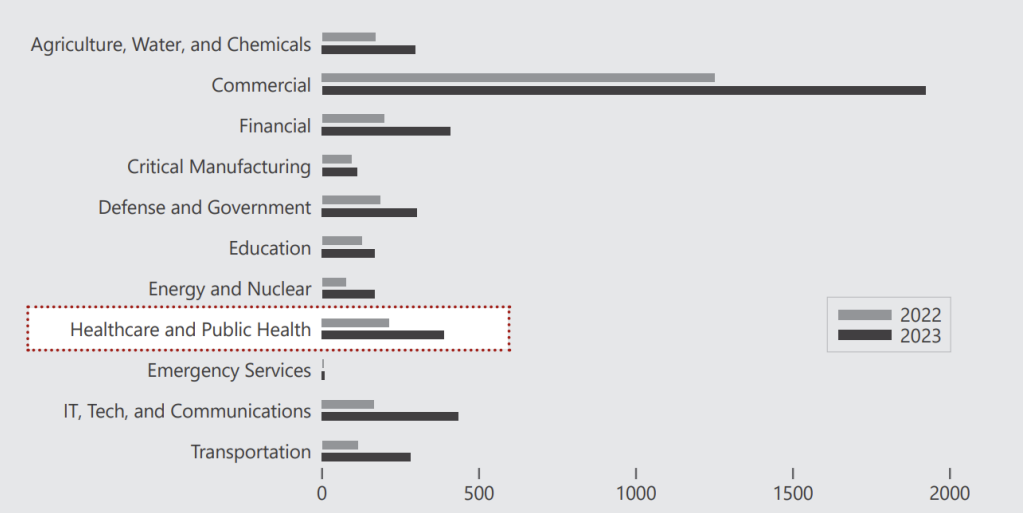
   a. Identificación de Activos Críticos: Lista de los sistemas de información, aplicaciones, bases de datos y equipos críticos para las operaciones del hospital.
      - Inventario de sistemas y datos: Se Lista todos los sistemas de información, aplicación, bases de datos, hardware y equipos críticos para las operaciones del Hospital.
        - Registro electrónico de salud:
        - Sistemas de monitoreo de pacientes
        - Equipos médicos conectados
        - Sistemas de Gestión Hospitalaria
        - Sistemas de comunicación
        - Servidores y Redes
        - Sistemas de Seguridad como firewalls y sistemas de detección de intrusos
      - Clasificación de activos
        - Críticos (nivel 1): Cuando afecta directamente la atención al paciente.

- Importantes (nivel 2): Afectar operaciones hospitalarias, pero no compromete inmediatamente la atención del paciente
- Soporte (nivel 3): Tienen un impacto menor a corto plazo.

b. Identificación de amenazas
   - Amenazas internas
     - Errores humanos: Personal que puede caer en ataques de phishing o cometer errores que comprometen a la seguridad del hospital.
     - Acceso no autorizado: Empleados con acceso en áreas restringidas que comprometan intencionalmente o no los sistemas.
     - Falta de capacitación: Personal que no se les dio un entrenamiento adecuado y por lo mismo no tiene prácticas de seguridad y de cómo mantener protegidos los sistemas y a ellos mismos.
   - Amenazas Externas
     - Ataques ransomware
     - Phishing
     - Ataques de fuerza bruta

c. Evaluación de vulnerabilidades
   - Análisis técnico: Utilizar herramientas para identificar sistemas sin parches o configuraciones inseguras, así mismo simular ataques para identificar puntos débiles.
   - Evaluación de procesos: Evaluar si las políticas actuales son adecuadas y se aplican correctamente.

d. Análisis de probabilidad e impacto
   - Probabilidad de ocurrencia: Tomando en cuenta que los ataques han aumentado del 2022 con 214 y en 2023 con 389 víctimas del ransomware en el área de cuidado de salud y salud publica según la Gráfica no.1



Gráfica No.1 COMPARISON OF TOTAL RANSOMWARE ATTACKS WORLDWIDE BY SECTOR, 2022 VERSUS 2023, Office of the Director of National Intelligence. (2023).

- Impacto potencial
  - Seguridad de paciente
  - Administrativo
  - Operacional
  - Financiero
  - Reputacional

e. Documentación y reporte
   Documentar todos los hallazgos, conclusiones y recomendaciones en un informe formal y presentar los resultados a la alta dirección para obtener apoyo, recursos y una solución.

2. Análisis del impacto en el Negocio (BIA)

Determinar el impacto potencial de los riesgos identificados en las operaciones críticas del hospital.

a. Identificación de funciones y procesos críticos
   - Atención al paciente:
     - Servicios de emergencia: Atención inmediata a situaciones críticas
     - Salas de parto y maternidad: Estos servicios son de alta importancia por lo que necesitan encontrarse siempre activos. La indisponibilidad de sistemas de monitoreo podría impedir detectar signos vitales críticos, poniendo en riesgo a los pacientes.

    - Unidades de cuidados intensivos: Esta unidad se encarga del tratamiento de pacientes en estado crítico y depende de sistemas para monitorear constantes vitales y administrar tratamientos de manera precisa.
- Sistemas clínicos:
    - Registros médicos electrónicos: Los registros médicos son fundamentales para un tratamiento adecuado y para la continuidad en la atención. Una interrupción en esta área afectaría la disponibilidad de información médica crítica.
    - Sistemas de diagnóstico y laboratorio: Permiten realizar diagnósticos precisos y de manera rápida. Su interrupción ralentizaría la capacidad de diagnóstico y afectaría el tratamiento oportuno.

b. Evaluación de impacto

- Seguridad y salud del paciente:
    - Riesgo inmediato: Interrupción de sistemas que monitorean signos vitales.
    - Riesgo a largo plazo: Pérdida de historiales médicos que afectan tratamientos futuros.
- Operacional:
    - Retrasos en procedimientos: Aumento de tiempos de espera.
    - Carga adicional de personal: Estrés y posibilidad de errores al usar procesos manuales.
- Legal y reputacional:
    - Demandas por negligencia.
    - Pérdida de confianza.
- Financiero:
    - Costos de recuperación: Gastos en restauración de sistemas y datos.
    - Pérdida de ingresos: Cancelación de procedimientos, reducción de pacientes.

c. Priorización de funciones y sistemas

- Máxima prioridad
    - Monitoreo de pacientes.
    - Sistemas de emergencia y Unidades de Cuidados Intensivos.

- Alta prioridad
    - Registros electrónicos de salud y sistemas de diagnóstico.
    - Comunicación interna para personal médico.
- Media prioridad
    - Sistemas administrativos y de facturación.

d. Análisis de dependencias
- Dependencias técnicas:
    - Registros electrónicos de salud dependen de la red y servidores.
    - Sistemas de monitoreo conectados a infraestructura de TI.
- Dependencias operacionales
    - Procedimientos médicos dependen de acceso a historiales.

e. Documentación del BIA
- Informe detallado:
    - Descripción de procesos críticos y su impacto.
    - RTO y RPO asignados.
    - Plan de priorización para recuperación.

3. Desarrollo del Plan de Continuidad del Negocio y Recuperación ante Desastres (BC/DR)

Identificación y Definición de Equipos de BC/DR y Personal Clave

Equipos especializados en cada una de las áreas, en donde se asignan roles y responsabilidades claras para la gestión de las fases del plan.

a. Equipo de Gestión de Crisis (CMT)
- Directivos de alto nivel, líderes de áreas críticas (TI, operaciones clínicas, recursos humanos, legal, comunicaciones).
- Responsabilidades:
    - Toma de decisiones durante crisis.
    - Coordinación de recursos y acciones entre los diferentes equipos.
    - Autorización de activación de plan BC/DR.
    - Actuar como punto de contacto principal con entidades externas.

b. Equipos de Respuesta a Incidentes de TI (CIRT)
- Especialistas en seguridad informática, administradores de sistemas y redes, expertos en recuperación de datos.

- Responsabilidades:
    - Detectar y analizar el alcance del ataque.
    - Contener y erradicar la amenaza.
    - Restaurar sistemas y servicios afectados.
    - Implementar medidas para prevenir futuros incidentes.

c. Comunicación de Crisis
    - Profesionales de comunicación y relaciones públicas, representantes de recursos humanos
    - Responsabilidades:
        - Gestionar la comunicación interna y externa durante la crisis.
        - Elaborar mensajes clave y comunicados de prensa.
        - Coordinar la información que se proporciona a pacientes, familiares, empleados y medios de comunicación.

d. Equipo de Apoyo Clínico
    - Personal médico y de enfermería clave, líderes de departamentos clínicos.
    - Responsabilidades:
        - Garantizar la continuidad de la atención al paciente.
        - Implementar procedimientos alternativos en caso de fallo de sistemas clínicos.
        - Coordinar la asignación de recursos clínicos durante la crisis.

e. Equipo de Recursos Humanos
    - Responsabilidades:
        - Manejar el bienestar y las necesidades del personal
        - Proporcionar el apoyo y recursos al personal afectado
        - Coordinar la reubicación del personal si es necesario
        - Acción rápida para la contratación de nuevo personal.

f. Equipo Legal y de Cumplimiento
    - Responsabilidades:
        - Asesorar sobre implicaciones legales y normativas
        - Garantizar el cumplimiento de las leyes y regulaciones que se aplicación en dentro del Estado.
        - Manejar la comunicación con las autoridades reguladoras, protegiendo siempre al establecimiento.

- El cumplimiento y la ejecución correcta de cada una de las leyes estipuladas.

g. Equipo de Seguridad Física
   - Responsabilidades:
     - Proteger las instalaciones y al personal
     - Controlar el acceso a áreas críticas durante la crisis, para mantener al personal controlado.
     - Coordinar con fuerzas de seguridad si es necesario.

Roles y Responsabilidades

- Líder del CMT: Director General
  - Sub-Líder: Gerente General
- Coordinador CIRT: Jefe de Seguridad Informática
  - Sub-Coordinador: Especialista en Respuesta a Incidentes
- Portavoz Oficial: Miembro designado del equipo de comunicación

Definición de Tareas y Asignación de Recursos

Detallamos las tareas especificas que cada equipo y miembro debe de realizar antes, durante y después del incidente.

<u>Actividades Previas al Incidente (Preparación):</u>

a. Implementación de Estrategias de Mitigación:
   - Equipo de TI:
     - Tener actualizado y parchear todos los sistemas y software.
     - Implementar soluciones de seguridad avanzadas como firewalls, antivirus e IDS/IPS
     - Configurar y probar sistemas de respaldo y recuperación de datos.
   - Equipo de Recursos Humanos:
     - Desarrollar y ejecutar programas de formación y concienciación en seguridad para todo el personal.
   - Equipo de Apoyo Clínico:
     - Desarrollar procedimientos alternativos manuales para operaciones clínicas críticas.
     - Asegurar la disponibilidad de equipos médicos esenciales en caso de fallo de sistemas.

b. Preparación de Recursos:
   - Inventario de Recursos:
     - Listar y asegurar la disponibilidad de recursos tecnológicos, humanos y logísticos necesarios.
   - Contratos con Proveedores:
     - Establecer acuerdos con proveedores de servicios de emergencia, recuperación de datos y soporte técnico.

c. Documentación y Procedimientos:
   - Desarrollo de Protocolos:
     - Crear procedimientos detallados para la activación del plan, respuesta a incidentes y recuperación.
     - Elaborar listas de verificación para tareas críticas.

<u>Actividades durante el Incidente (Respuesta Inmediata)</u>

a. Activación del Plan

Criterios de activación (Triggers)

Definir eventos específicos que justifican la activación inmediata del plan de continuidad del Negocio y Recuperación ante desastres.

- Detección de actividades maliciosas en el sistema
  - Alerta de Antivirus o sistemas de detección de intrusos que indican la presencia de un ransomware.
  - El comportamiento inusual en sistemas, como encriptación de archivos, creación de archivos desconocidos o cambios repentinos en la configuración de nuestro sistema.
  - Usuarios reportan mensajes de rescate o solicitudes de pago para la recuperación de archivos
  - La respuesta lenta de los sistemas debe de estar siempre actualizado a la última versión.
- Interrupción Repentina de Sistemas Críticos
  - Caída del sistema de registros médicos electrónicos, sistemas de monitoreo de pacientes o aplicaciones clínicas críticas. Imposibilidad de acceder a la base de datos o archivos esenciales para la atención y seguimiento de los pacientes.
- Anomalías en el tráfico de red
  - El aumento inusual del trafico de red saliente, indicando la posible exfiltración de datos y conexiones a direcciones IP o dominios sospechosos y no autorizados.

- Reportes del personal sobre problemas técnicos
    - Múltiples empleados reportan problemas con el acceso o funcionamiento de los sistemas de uso diario en el Hospital.
- Notificación de proveedores o entidades externas
    - Alertas de proveedores de seguridad sobre amenazas y advertencias de autoridades o agencias de seguridad cibernética sobre un posible ataque.

Procedimientos para la evaluación del incidente

Pasos claros para la evaluación rápida de la situación y confirmación de la necesidad de activar el plan

Paso 1: Recepción de la alerta
Responsable: Personal de TI o seguridad cibernética que detecte el incidente
Acción: Documentar la alerta inicial y cualquier información que sea relevante (Fecha, Hora, Sistemas Afectados, daños críticos y el inicio del posible problema).

Paso 2: Notificación inmediata al Líder del CIRT
Responsable: Personal que detecto el incidente
Acción: Contactar con el líder del CIRT (teléfono, mensaje de texto o canal designado), si no se encuentra se adjunta también el sublíder de CIRT. Luego de contactar con el líder se debe de proporcionar detalles preliminares.

Paso 3: Evaluación técnica Inicial
Responsable: Encargado del CIRT
Acción: Reunirse para analizar la información disponible hasta el momento y verificar la legitimidad y gravedad de la amenaza, así mismo determinar el alcance preliminar.

Paso 4: Determinación de Activación del plan
Responsable: Líder del CIRT con la coordinación del director de TI y encargado de la seguridad cibernética.
Acción: Si se confirma el incidente que cumple con los criterios de activación se recomienda la activación del plan al líder de CMT

Paso 5: Autorización de Activación
Responsable: Líder del CMT
Acción: Autorizar formalmente la activación del plan BC/DR. Instruir a los equipos para proceder con los protocolos establecidos.

b. Notificación y Planificación

Equipo de gestión de crisis (CMT)

Notificar a todas las partes afectadas a reuniones de emergencia para poder coordinar la respuesta al incidente

Paso 1: Activación del CMT
Responsable: Líder del CMT
Acción: Utilizar el sistema de notificación de emergencias para poder contactar a todos los miembros del CMT y proporcionarles información breve sobre el incidente y hora/lugar de la reunión de emergencia.

Paso 2: Convocatoria de reuniones de Emergencia
Responsable: Líder del CMT
Acción: Asegurar que todos los miembros tengan los medios para asistir

Paso 3: Preparación de información inicial
Responsable: Líder del CIRT
Acción: Preparar un informe preliminar del incidente para presentarlo al CMT, en donde se incluyan detalles sobre sistemas afectados y acciones inmediatas recomendadas.

Equipo de comunicación

Informar al personal sobre el incidente y proporcionar instrucciones claras para preparar a los pacientes y público en general si es necesario.

Paso 1: Activación del equipo de comunicación
Responsable: Director de comunicación y relaciones públicas.
Acción: Notificar a todos los miembros del equipo y asignar roles.

Paso 2: Elaboración de mensajes internos
Responsable: Equipo de comunicación en coordinación con CMT
Acción: Descripción general del incidente. Instrucciones claras sobre que hacer (no apagar equipos, no conectar dispositivos externos) e informar sobre cómo se mantendrá la comunicación.

Paso 3: Difusión del mensaje al personal

Responsable: Equipo de comunicación
Acción: Utilizar canales de comunicación internos en donde se aseguren de hacer llegar el mensaje a todo el personal, incluidos aquellos sin acceso regular a correo electrónico.

Paso 4: Preparación de mensajes para pacientes y público en general
Responsable: Equipo de comunicación con CMT y Asesor legal.
Acción: Evaluar si es necesario informar a pacientes y publico externo, si se decide comunicar preparar mensajes que tranquilicen al público sobre las medidas que se están tomando, información sobre cómo podrían versea afectados los servicios y no revelar información sensible o detalles que comprometan la seguridad.

Paso 5: Gestión de Medios de Comunicación
Responsable: Portavoz designado
Acción: Preparar las declaraciones oficiales y coordinar cualquier interacción con medios de comunicación.

c. Respuesta técnica

Aislar sistemas afectados, analizar el alcance y origen del incidente, implementando medidas de contención y comenzar con los procedimientos de recuperación

Procedimientos

a. Aislamiento de Sistemas Afectados
    i. Desconectar sistemas comprometidos
        a) Desconectar de la red los sistemas identificados como afectados para evitar la propagación, esto puede incluir desde servidores, estaciones de trabajo o dispositivos de almacenamiento
    ii. Seguridad de Datos
        a) Evitar apagar los sistemas a la fuerza, si es posible aislarlos de la red y documentar acciones tomadas para fines de análisis.

b. Análisis del Alcance y Origen del Incidente
    i. Recolección de información
        a) Analizar los registros de los sistemas infectados, firewalls, IDS/IPS para identificar cualquier actividad sospechosa.
        b) Determinar cómo ingreso el atacante
    ii. Evaluación de impacto

a) Crear un listado con el inventario de todos los sistemas comprometidos y determinar si hubo acceso o robo de información sensible.

c. Implementación de medidas de contención
    i. Bloqueo de accesos no autorizados
        a) Bloquear direcciones IP, puertos o protocolos utilizados por el atacante y cambiar las contraseñas y deshabilitar cuentas de usuarios afectadas.
    ii. Escaneo de sistemas
        a) Utilizar herramientas de escaneo para identificar malware conocido y comparar hashes de archivos críticos con copias de referencia,

d. Procedimientos de recuperación
    i. Restauración de sistemas
        a) Asegurar que las copias de seguridad no estén comprometidas.
        b) Priorizar la recuperación de sistemas definidos como críticos en el BIA
        c) Actualizar sistemas para corregir vulnerabilidades explotadas
        d) Revisar configuraciones de seguridad y reforzar donde sea necesario.

e. Comunicación con Otros equipos
    i. Informes al CMT
        a) Proporcionar informes sobre el progreso de la contención y recuperación
        b) Asesorar sobre acciones adicionales
        c) Comunicar cuando los sistemas clínicos están disponibles nuevamente y ayudar al personal clínico en la transición de procedimientos manuales a sistemas restaurados

d. Continuidad de operaciones clínicas

Implementar procedimientos manuales o alternativos para mantener la atención al paciente, priorizando recursos y coordinar con otros departamentos.

Procedimientos

a. Implementación de procedimientos manuales o alternativos
    i. Uso de protocolos de contingencia
    Emplear formularios preimpr4esos para documentación clínica y utilizar equipos portátiles o manuales.

ii. Instrucciones al personal clínico
Brindar recordatorios o capacitación breve sobre procedimientos manuales, designar al personal para tareas específicas, como manejo de registro en papel coordinación de pacientes.

b. Priorización de recursos
   i. Identificar pacientes en estado crítico que requieren atención prioritaria y asegurar que haya suficiente personal calificado asignado a áreas críticas.
   ii. Verificar la disponibilidad de medicamentes y equipos esenciales y coordinar con el almacén y proveedores para evitar escasez.

c. Colaboración con IT
   i. Mantenerse informados sobre el estado de los sistemas clínicos y comunicar cualquier dificultad o necesidad técnica al CIRT.
   ii. Solicitar personal adicional si es necesario

d. Documentación y registro
   i. Asegurar que todos los procedimientos y atención brindada sean documentados adecuadamente en papel
   ii. Planificar como se ingresará la información en sistemas electrónicos una vez restaurados
   iii. Almacenar registros en lugares seguros para evitar perdida o acceso no autorizado
   iv. Asegurar que los procedimientos manuales cumplen con regulaciones de privacidad y confidencialidad

e. Soporte al personal clínico
   i. Establecer puntos de contacto para que el personal pueda hacer consultas o reportar problemas

4. Implementación y Entrenamiento

Capacitar al personal, probar el plan y realizar auditorías periódicas.

a. Desarrollo de programas de entrenamiento
   - Identificación de necesidades:
     - Análisis de Roles y responsabilidades: Determinar las competencias requeridas para cada rol durante una crisis. Identificar brechas de conocimiento en seguridad cibernética y procedimientos de emergencia.

- Diseño de contenido:
    - Módulos específicos: Seguridad cibernética (amenazas comunes como ransomware, pishing). Buenas prácticas y protocolos de reporte.
    - Procedimientos de emergencia: Activación del plan BC/DR. Roles y responsabilidades durante una crisis. Protocolos de comunicación interna y externa.

b. Capacitación del personal
    - Sesiones regulares
        - Personal clave (CMT, CIRT, líderes, clínicos): Entrenamientos profundos y frecuentes (trimestrales, semestrales). Enfoque en liderazgo, toma de decisiones y gestión de crisis.
        - Personal general: Formación básica inicial y actualizaciones anuales. Enfoque en procedimientos de emergencia y seguridad cibernética básica.
    - Métodos de entrenamiento
        - Teórico: Presentaciones, lecturas y sesiones informativas.
        - Práctico: Simulaciones y ejercicios de roles. Uso de equipos y procedimientos en entornos controlados.

c. Pruebas del plan
    - Ejercicios en papel (walk-throughs): Revisiones teóricas del plan con los equipos involucrados. Discusión de escenarios hipotéticos y acciones correspondientes.
    - Ejercicios funcionales: Simulaciones prácticas de incidentes específicos (ataques de ransomware). Evaluación de la respuesta del personal y eficiencia de los procedimientos.
    - Simulacros de campo: Pruebas en entornos controlados que involucren restauración de sistemas desde respaldo y operaciones clínicas utilizando procedimientos manuales.

d. Evaluación y retroalimentación
    - Medición de resultados: Evaluar el desempeño del personal durante entrenamientos y simulacros. Utilizar indicadores como tiempo de respuesta y adherencia a protocolos.
    - Lecciones aprendidas: Identificar fortalezas y áreas de mejora. Actualizar el plan y los programas de capacitación según los hallazgos.

e. Auditorías periódicas
   - Auditorías internas: Revisiones regulares del cumplimiento y efectividad del plan BC/DR. Evaluación de políticas de seguridad y preparación del personal.
   - Auditorías externas: Contratación de terceros para evaluaciones independientes. Asegurar el cumplimiento con regulaciones y estándares del sector de salud.

5. Mantenimiento y Mejora continua

Evaluación de la Respuesta al Incidente

Mantenimiento: Realizar revisiones periódicas de los procedimientos de respuesta ante incidentes, como desconexión de redes y notificación a las autoridades. Esto incluye practicar simulacros para medir la eficiencia y actualizar los protocolos según los últimos aprendizajes.

Mejora Continua: Implementar auditorías después de cada incidente o simulacro para identificar y documentar áreas de mejora. Comparar las prácticas actuales con las mejores prácticas en recuperación ante desastres para introducir mejoras, como adoptar tecnologías de recuperación automatizada y segmentación de redes, etc.

Mejora de Procedimientos de Comunicación

Mantenimiento: Actualizar constantemente las herramientas de comunicación de emergencia y capacitar al personal en su uso. Realizar simulaciones de crisis para mantener al equipo preparado en el uso de estas herramientas.

Mejora Continua: Después de cada simulacro o incidente real, analizar la efectividad de la comunicación y realizar ajustes necesarios. Establecer métricas claras para evaluar la rapidez y claridad en la comunicación, mejorando según los resultados.

Preparación Continua

Mantenimiento: Realizar evaluaciones de riesgo y análisis de impacto en el negocio (BIA) de manera regular para asegurarse de que las vulnerabilidades y amenazas estén actualizadas y documentadas.

Mejora Continua: Utilizar los hallazgos de cada evaluación y simulacro para actualizar los planes de continuidad del negocio (BC/DR). Incluir en el BIA los cambios en los procesos críticos y ajustarlos en función de los nuevos riesgos identificados.

Conclusiones

- Es fundamental establecer vías de comunicación efectivas y claras durante crisis, como los ciberataques. Es crucial que el personal esté informado de manera oportuna y transparente para minimizar la confusión y asegurar que puedan desempeñar sus funciones de manera segura
- Las organizaciones deben reforzar su infraestructura de ciberseguridad para proteger sus sistemas de amenazas como el ransomware.
- Los procedimientos médicos y la toma de decisiones deben mantenerse firmes, incluso en situaciones de emergencia tecnológica. La ausencia de sistemas digitales no debe afectar la atención médica.
- Es crucial contar con una buena seguridad en los sistemas y una infraestructura robusta para garantizar el correcto funcionamiento de los hospitales y la seguridad de los pacientes, especialmente en situaciones críticas

Anexos

Bibliografía

Westcon-Comstor, E. S. (2021, 24 septiembre). 5 mejores prácticas de recuperación ante desastres para evitar fallas y vulnerabilidades. *LAC BLOG*. https://blog-es.lac.tdsynnex.com/5-mejores-practicas-de-recuperacion-ante-desastres-para-evitar-fallas-y-vulnerabilidades

Office of the Director of National Intelligence. (2023). *Ransomware attacks surge in 2023*. https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf

El coste del ransomware: ¿por qué todas las empresas pagan de una forma u otra? (2023, 31 mayo). Acronis. https://www.acronis.com/es-es/blog/posts/cost-of-ransomware/#:~:text=Despu%C3%A9s%20de%20un%20incidente%20de%20ransomware%2C%20el%20negocio,50%20veces%20m%C3%A1s%20que%20la%20demanda%20de%20rescate.