**Guía Integral de Preparación y Respuesta ante Ransomware en el Sector Salud: Políticas, Lineamientos y Mejores Prácticas**

Para preparar a una empresa del sector salud ante la amenaza del ransomware, es fundamental desarrollar un enfoque estructurado que aborde tanto la prevención como la respuesta a incidentes.

**Acciones Inmediatas para Comenzar**

1. Realiza un diagnóstico inicial de riesgos.
2. Diseña un plan de capacitación para la gerencia.
3. Desarrolla y aprueba las políticas de respuesta ante ransomware.
4. Implementa pruebas de restauración y simulaciones de incidentes.
5. Actualiza el plan según lecciones aprendidas.

DESARROLLO

**1. Evaluación y Diagnóstico Inicial**

* Evaluación de Riesgos:
  + Realiza un análisis de vulnerabilidades y un assessment de riesgos enfocado en ransomware. Identifica los sistemas críticos, especialmente los que manejan datos sensibles de pacientes (PHI) y sistemas de registro electrónico de salud (EHR).
  + Evalúa la exposición a través de terceros (proveedores, contratistas) y posibles vectores de ataque (phishing, RDP, vulnerabilidades no parchadas).
* Clasificación de Datos y Sistemas:
  + Prioriza la protección de datos confidenciales y sistemas esenciales para la continuidad del servicio de salud.

**2. Concienciación y Capacitación del Personal de Gerencia**

* Capacitación para la Alta Dirección:
  + Realiza talleres específicos para gerentes y ejecutivos sobre:
    - Impacto financiero y legal del ransomware en el sector salud.
    - Roles y responsabilidades en caso de un ataque.
    - Importancia de respaldos y políticas de ciberseguridad.
* Simulaciones de Incidentes (Tabletop Exercises):
  + Organiza simulaciones de ransomware para el equipo de liderazgo y gestión de crisis.
  + Evalúa la capacidad de toma de decisiones bajo presión y la coordinación con los equipos técnicos.

**3. Desarrollo de Políticas y Lineamientos Específicos**

* Política de Respuesta ante Ransomware:
  + Define qué hacer y quién hace qué en cada etapa del ataque.
  + Establece criterios para notificar a las autoridades (en Perú, Ley de Protección de Datos Personales) y a los afectados.
* Política de Respaldo y Restauración:
  + Especifica frecuencia de backups, ubicación de respaldos (on-premises y cloud) y pruebas periódicas de restauración.
  + Asegúrate de que los respaldos estén desconectados (air-gapped) del entorno principal.
* Política de Actualización y Parches:
  + Establece plazos claros para parchar vulnerabilidades críticas.
  + Asegúrate de que el software y hardware médico tengan un plan de actualización.

**4. Prevención y Fortalecimiento de la Postura de Seguridad**

* Chequeo de Salud y Seguridad de Active Directory (AD):
  + Revisar que no existan problemas de replicación ni errores en los controladores de dominio.
  + Identificar cuentas con privilegios excesivos y eliminar accesos no necesarios.
  + Revisar contraseñas antiguas o cuentas inactivas.
  + Evaluar políticas de seguridad, como bloqueos de cuentas y contraseñas complejas.
  + Revisar cambios recientes y asegurar la integridad de GPOs críticas.
  + Revisar eventos sospechosos, accesos inusuales y fallos de inicio de sesión.
  + Asegurarse de que el sistema operativo y el software del AD estén actualizados.
* Autenticación y Acceso:
  + Implementa autenticación multifactor (MFA) para todo acceso remoto y sistemas críticos.
  + Limita el uso de protocolos inseguros como RDP expuesto a Internet.
* Protección de Endpoints y Redes:
  + Usa soluciones de EDR/XDR y herramientas de detección y respuesta ante amenazas.
  + Segmenta la red para minimizar el impacto de un ataque.
  + Monitorea y bloquea actividades sospechosas (movimiento lateral, cifrado masivo).
* Phishing y Concienciación del Usuario:
  + Capacita regularmente al personal en detectar y reportar correos maliciosos.
  + Realiza simulaciones de phishing para medir la resiliencia.

**5. Plan de Respuesta a Incidentes (IRP)**

* Estructura del Plan:
  + Define claramente las fases de detección, contención, erradicación y recuperación.
  + Establece procedimientos para aislar sistemas afectados y minimizar la propagación.
* Equipo de Respuesta ante Incidentes (CSIRT):
  + Crea un equipo multidisciplinario (IT, legal, comunicaciones, recursos humanos) para gestionar crisis.
* Plan de Comunicación:
  + Diseña un plan para comunicar el incidente a las partes interesadas (pacientes, reguladores, prensa).

**6. Recuperación y Mejora Continua**

* Pruebas de Restauración:
  + Verifica periódicamente la capacidad de restaurar datos y sistemas a partir de backups.
  + Realiza auditorías para asegurar que los sistemas parchados y los accesos estén actualizados.
* Lecciones Aprendidas:
  + Después de cada simulación o incidente, documenta las lecciones aprendidas y actualiza las políticas.

Recomendaciones Específicas para el Sector Salud

* Cumplimiento Legal y Normativo:
  + Considera los estándares de HIPAA, y la normativa de protección de datos personales en Perú.
* Ciberseguro (Cyber Insurance):
  + Evalúa la posibilidad de contar con un seguro de ciberseguridad para mitigar el impacto financiero.

Referencias

* Cybersecurity and Infrastructure Security Agency (CISA). (2020). *Ransomware Guide*. CISA.  
  https://www.cisa.gov/sites/default/files/publications/CISA\_MS-ISAC\_Ransomware\_Guide\_S508C.pdf
* National Institute of Standards and Technology (NIST). (2020). *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events (NIST SP 1800-26)*. U.S. Department of Commerce.  
  <https://csrc.nist.gov/publications/detail/sp/1800-26/final>
* Health Sector Cybersecurity Coordination Center (HC3). (2021). *Ransomware Trends 2021: Risks to the Healthcare Sector*. U.S. Department of Health and Human Services (HHS).  
  https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf
* Microsoft Security Intelligence. (2022). *Ransomware Protection Best Practices*. Microsoft.  
  <https://www.microsoft.com/security/blog>
* European Union Agency for Cybersecurity (ENISA). (2021). *Threat Landscape for Ransomware Attacks*. ENISA.  
  <https://www.enisa.europa.eu/publications/threat-landscape-for-ransomware-attacks>
* Verizon. (2023). *Data Breach Investigations Report (DBIR) 2023*. Verizon Enterprise.  
  https://www.verizon.com/business/resources/reports/dbir/
* IBM Security. (2022). *Cost of a Data Breach Report 2022*. IBM Security.  
  https://www.ibm.com/security/data-breach
* Kaspersky Lab. (2021). *Ransomware Attacks in Healthcare: Trends and Mitigation Strategies*. Kaspersky.  
  https://www.kaspersky.com/resource-center/threats/ransomware
* Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI). (2020). *Guía de Buenas Prácticas en Seguridad de la Información y Protección de Datos*. INDECOPI, Perú.  
  https://www.indecopi.gob.pe/
* International Association of Privacy Professionals (IAPP). (2022). *Ransomware and Data Breaches in Healthcare: Legal Implications*. IAPP.  
  <https://iapp.org/>