**Riesgo:** Utilizando la técnica de Phishing una persona externa a la organización logra obtener datos de pacientes y registrar turnos aleatoriamente, generando la saturación de los turnos.

**INVENTARIO DE ACTIVOS**

**Escalas de valores:**

1. Muy bajo, 2. Bajo, 3. Medio, 4. Alto, 5. Muy alto

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **ACTIVO** | **TIPO** | **CONTENEDOR** | **RELACIONADOS** | **DUEÑO** | **CUSTODIO** | **C** | **I** | **D** | **Crit.** |
| 1 | Proceso de Atención Ambulatoria | Proceso |  |  | Jefe de Atenciones Ambulatorias | Empleados de Atención Ambulatoria  Enfermeras  Médicos de Atención Ambulatoria | 5 | 5 | 5 | 15 |
| 2 | Sistema sanatorial | Software | Servidor | 1,3,4,5 | Jefa de Sistemas | Empleados de Sistemas, Usuarios del Sistema Sanatorial | 5 | 5 | 5 | 15 |
| 3 | Turnos | Información | Base de Datos del Sistema Sanatorial | 1,2,4 | Paciente | Empleados de Atención Ambulatoria  Enfermeras  Médicos de Atención Ambulatoria | 3 | 3 | 5 | 11 |
| 4 | BD del Sistema Sanatorial | Información | Servidor | 5 | Jefa de Sistemas | Personal de Sistemas | 4 | 5 | 5 | 13 |
| 5 | Servidor | Hardware | Instalaciones del Departamento de Sistemas |  | Jefa de Sistemas | Personal de Sistemas | 3 | 5 | 5 | 13 |

**IDENTIFICACIÓN DE RIESGOS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Id.** 01 |  | | | |
| **Identificador** |  |  | | |
| **Especificación** | Utilizando la técnica de Phishing una persona externa a la organización logra obtener datos de pacientes y registrar turnos aleatoriamente, generando la saturación de los turnos. | | | |
| **Clasificación** | **2. Fallas de Sistemas y Tecnología** | | **2.2 Software** | **2.2.4.Parámetros de seguridad** |
| **Contexto** | | | | |
| **Descripción** | El atacante utiliza una técnica de ingeniería social logrando obtener datos de pacientes. De esta forma tiene la posibilidad de acceder al sistema para registrar turnos.  En el contexto no se especifica si el sistema de turnos envía alguna alerta a la cuenta de mail registrada del paciente. Sin embargo, aunque lo hiciera, es posible que el paciente se de cuenta días después de que sus datos han sido utilizados para generar turnos.  Tampoco se especifica si el software de turnos cuenta con un sistema de alertas que analice la generación masiva de turnos en un determinado período de tiempo. | | | |
| **Valoración del Riesgo** | | | | |
| **Factores para evaluar la magnitud de pérdida**  **Activos**: En la planilla de activos se ha establecido el nivel de criticidad de los activos afectados. Además, se pueden considerar:   * **Productividad**: la productividad se ve afectada ya que el sanatorio no puede dar de baja ni cambiar el estado de los turnos, eso es potestad del dueño (en este caso el paciente) que sólo estará en condiciones de cancelarlos en caso de que se le haya enviado una alerta para la confirmación de turnos. Esta saturación trae aparejada la imposibilidad de otorgar los turnos a pacientes reales que lo estén necesitando hasta tanto se verifique el ataque. * **Costo de reemplazo**: El costo de restablecer los turnos a un estado correcto. * **Sensibilidad**:   + **Reputación:** Puede afectar la imagen del sanatorio el hecho de que el/los pacientes afectados reciban correos masivos de generación de turnos   + **Ventaja competitiva**: Puede ser utilizado por la competencia para perjudicar la imagen del sanatorio   + **Legal / Regulatoria:** Se ha realizado un uso indebido de los datos de pacientes (que pueden no ser sensibles pero que son los que se requieren para generar los turnos).   + **General**: No aplica * **Volumen:** Dependerá, en este caso, de la cantidad de pacientes afectados y de la cantidad de turnos generados hasta la detección de la materialización del riesgo.   **Amenazas:** la generación masiva de turnos constituye la amenaza al proceso, el phishing constituye la amenaza que hay que contrarrestar en este caso para que los pacientes no cedan sus datos   * **Competencia:** No aplica (Si bien podría pensarse que el atacante es una institución de la competencia) * **Internas/Externas:** La amenaza es externa y atenta sobre una persona que no conforma parte de los recursos humanos de la organización. No se puede actuar directamente sobre la amenaza(el atacante) ni sobre la vulnerabilidad que explota (confianza del paciente al ceder sus datos). Solo puede actuarse sobre el incidente (detección de generación masiva de turnos) * **Acción:**   + **Acceso**: El atacante accede a los sistemas de la organización   + **Uso indebido:** Hace uso indebido de los datos para obtener acceso y registrar turnos   + **Divulgación:** Tendría la posibilidad de divulgar los datos de los pacientes afectados.   + **Modificación:** Realiza modificación (en este caso registro) de datos afectando la integridad de la información   + **Denegación de acceso**: podría considerarse también una denegación de acceso ya que la generación de turnos masivamente produce que otros pacientes se queden sin la posibilidad de tomar turnos   **Organización:** El riesgo se desarrolla fuera del contexto del sanatorio y ocasiona la pérdida de la capacidad de operar normalmente   * **Momento**: Los turnos son la herramienta que utiliza el sanatorio para el acceso a las prestaciones ambulatorias por lo que la no resolución en tiempo y forma del incidente tendría un impacto de pérdida alto (muchos pacientes podrían optar por otros prestadores al no conseguir los turnos requeridos) * **Debido cuidado:** No se especifican en el contexto mecanismos que permitan resistir a este tipo de ataques. Amenazas de este tipo están en constante evolución por lo que habrá que mantener una vigilancia constante. * **Detección:** La detección podría realizarse en forma anticipada incluyendo mecanismos que detecten la generación de turnos en forma masiva. Un usuario del sistema sanatorial podría recibir la alerta de un paciente que quiere generar turnos y llama telefónicamente al no encontrar disponibilidad. Un usuario del sistema sanatorial podría verificar los turnos dados a un determinado paciente que no se presenta al turno dado. * **Respuesta:** No se especifica en el riesgo si la organización está preparada para operar ante la materialización del riesgo. En función de esto se puede analizar:   + **Contención**: Los usuarios finales no están capacitados para afrontar este tipo de problemas.   + **Remediación**: Eliminación de los turnos que no deberían haber sido generados   + **Recuperación**: Reanudación del proceso de atención.   **Factores externos:**   * **Detección:** La detección específica del atacante es difícil de realizar. Se debería disminuir el tiempo en que el atacante mantiene el acceso implementando estrategias como: envío de correos de confirmación o análisis para detectar la generación masiva de turnos y emisión de alarmas. * **Legal / Regulatorio**: Posible divulgación de datos sensibles de pacientes. * **Competidores**: En caso de filtración de datos, la competencia podría utilizarlos para su propio beneficio. * **Medios de comunicación**: Que el incidente sea conocido por medios de comunicación puede afectar la imagen de la organización (bajo). * **Otros grupos de interés:** No aplica   **Utilizando la escala de valores se puede decir que el impacto es: Alto (4).**  **Factores utilizados para el cálculo de la probabilidad:**  **Frecuencia de amenazas**:   * **Contacto**: El contacto de la amenaza es intencional por lo que buscará la forma de tomar contacto con el paciente para obtener sus datos y así generar turnos para saturar el sistema.   **Aleatorio: -- Regular**: **--** **Intencional**: **X**   * **Acción**: Materializada la amenaza de este riesgo el proceso se ve afectado en su operatoria normal. Se ven afectada la integridad y disponibilidad de los turnos   + **Beneficio**: personales del atacante. Por ejemplo puede ser competencia y querer obtener ventaja para que los pacientes busquen otras alternativas para su atención o simplemente “divertirse” o practicar sus habilidades como “cracker”   + **Nivel de esfuerzo**: Está dado por las habilidades del atacante en aplicar técnicas de Ingeniería Social.   + **Riesgo de detección**: Del atacante es muy bajo (no accede con sus propios datos, sólo podría detectarse en función de la IP desde donde materializa el ataque).   **Vulnerabilidades**: la obsolescencia del sistema sanatorial (y en particular el afectado: sistema de turnos).   * **Capacidad de las amenazas**: no requiere conocimientos especiales, sólo manipular al paciente para que ceda sus datos. * **Capacidad de resistencia**(CR): Muy Bajo. No existen estrategias implementadas para mitigar los efectos del ataque. Este tipo de amenazas se detecta una vez materializado, es decir una vez que el daño ya está hecho.   **Utilizando la escala de valores se puede decir que la probabilidad es: Alta (4).** | | | | |
| **Consecuencias** | Puede sufrir una pérdida monetaria grande ya que no puede continuar con el proceso hasta que se recupere el sistema de turnos. Posible pérdida de todos los pacientes que han querido tomar turnos y no han podido hacerlo hasta que se recupere el sistema | | | |
|  |  |  |  |  |

**TRATAMIENTO DE RIESGOS**

|  |  |  |
| --- | --- | --- |
| **Id.** 01 | |  |
| **Identificador** | |  |
| **Especificación** | | Utilizando la técnica de Phishing una persona externa a la organización logra obtener datos de pacientes y registrar turnos aleatoriamente, generando la saturación de los turnos. |
| **E S T**  **R A T E G I A S** | **Evitar** | |
| No se puede evitar el riesgo. Solo se podría si la vía de obtención de turnos fuera solo la telefónica donde el personal de admisión realice el registro de los turnos | |
| **Transferir** | |
| No se puede transferir. | |
| **Mitigar** | |
| Se establecen las siguientes estrategias para mitigar la probabilidad de ocurrencia:   1. Realizar concientización a los pacientes para la no entrega de datos que puedan ser utilizados como vía de acceso al sistema de turnos del sanatorio. 2. Agregar políticas y aplicación de contraseñas seguras (ej: doble factor de autenticación) al sistema de turnos   Se establecen las siguientes estrategias para mitigar el impacto:   1. Desarrollar confirmación vía correo electrónico, requiriendo confirmación inmediata de lo contrario se dará de baja el turno 2. Realizar controles automatizados de generación masiva de turnos (desarrollo por parte de la empresa tercerizada) | |
| **C O N**  **T**  **R**  **O**  **L**  **E**  **S** | Los controles que garantizan las estrategias de mitigación mencionadas son:   * Control de Accesos.   + Requisitos de negocio para el control de accesos.     - Política de control de accesos   + Control de acceso a sistemas y aplicaciones.     - Gestión de contraseñas de usuario. * Adquisición, Desarrollo y Mantenimiento de Sistemas   + Requerimientos de Seguridad de los Sistemas de Información   + Procesamiento correcto en Aplicaciones     - Validación de los datos de entrada     - Control de Procesamiento interno | |
| **Riesgo Residual** | | |
| Con las estrategias mencionadas se baja la probabilidad del riesgo a medio y el impacto a bajo. | | |

**PLANES DE CONTINGENCIA, RECUPERACIÓN Y CONTINUIDAD DE NEGOCIO**

|  |  |
| --- | --- |
| **Id.** 01 |  |
| **Identificador** |  |
| **Especificación** | Utilizando la técnica de Phishing una persona externa a la organización logra obtener datos de pacientes y registrar turnos aleatoriamente, generando la saturación de los turnos |
| **Disparadores** | 1. Paciente llama para quejarse porque no se pudo sacar turno en el sistema de turnos. 2. Paciente llama para registrar turno y el personal encargado de registrarlo no puede realizar la actividad. 3. Personal de admisión detecta la no presencia de paciente a un turno y revisa los turnos generados 4. Utilizando los controles previstos en las estrategias de mitigación:    1. Turnos registrados y dados de baja por no respuesta en tiempo del mail enviado de confirmación    2. Alarma por detección de generación masiva de turnos |
| **Contingencia** | En cualquier caso:   1. Se informa el incidente. 2. Se elimina la posibilidad de registrar turnos via el sistema indicando en su lugar que los turnos serán dados telefónicamente. |
| **Recuperación** | El personal de sistemas se encargará del tratamiento del incidente:   * Revisar los pacientes afectados * Dar de Baja los turnos que no correspondan * Poner nuevamente en funcionamiento el sistema. * Cierre del incidente |
| **Continuidad de Negocio** | Una vez detectado e informado el incidente todos los turnos serán registrados manualmente en planillas destinadas a tal fin |
| **Controles de Garantía de los Planes** | * Gestión de Incidentes en la seguridad de la información.   + Gestión de incidentes de seguridad de la información y mejoras.   + Responsabilidades y procedimientos.   + Notificación de los eventos de seguridad de la información.   + Notificación de puntos débiles de la seguridad.   + Valoración de eventos de seguridad de la información y toma de   + decisiones.   + Respuesta a los incidentes de seguridad.   + Aprendizaje de los incidentes de seguridad de la información.   + Recopilación de evidencias.   Evidencias objetivas: Documentación de la materialización del riesgo, documentación de los procedimientos de Contingencia, Recuperación y Continuidad de Negocio |