**Riesgo:** Posibilitado por un malware instalado en la máquina de un usuario, una persona externa a la organización logra obtener las claves de acceso de diferentes usuarios y registrar turnos aleatoriamente para diferentes pacientes, generando una sobreasignación y 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 | 1,3,4,5,6,7 | Jefa de Sistemas | Empleados de Sistemas, Usuarios del Sistema Sanatorial | 5 | 5 | 5 | 15 |
| 3 | Informes de Prácticas | Información | Base de Datos del Sistema Sanatorial | 1,5 | Paciente | Empleados de Atención Ambulatoria  Enfermeras  Médicos de Atención Ambulatoria | 5 | 5 | 5 | 15 |
| 4 | Turnos | Información | Base de Datos del Sistema Sanatorial | 1,2 | Paciente | Empleados de Atención Ambulatoria  Enfermeras  Médicos de Atención Ambulatoria | 3 | 3 | 5 | 11 |
| 5 | Historias clínicas | Información | Base de datos del Sistema Sanatorial | 1,2,3 | Paciente | Empleados de Atención Ambulatoria  Enfermeras  Médicos de Atención Ambulatoria | 5 | 5 | 3 | 13 |
| 6 | BD del Sistema Sanatorial | Información | Servidor | 7,8 | Jefa de Sistemas | Personal de Sistemas | 4 | 5 | 5 | 13 |
| 7 | Gestor de DB | Software | Servidor | 8 | Jefa | Personal de Sistemas | 1 | 5 | 5 | 11 |
| 8 | Servidor | Hardware | Instalaciones del Departamento de Sistemas |  | Jefa de Sistemas | Personal de Sistemas | 3 | 5 | 5 | 13 |

**IDENTIFICACIÓN DE RIESGOS**

| **Id.** 01 |  | | | |
| --- | --- | --- | --- | --- |
| **Identificador** |  |  | | |
| **Especificación** | Posibilitado por un malware instalado en la máquina de un usuario, una persona externa a la organización logra obtener las claves de acceso de diferentes usuarios y registrar turnos aleatoriamente para diferentes pacientes, generando una sobreasignación y saturación de los turnos | | | |
| **Clasificación** | **2. Fallas de Sistemas y Tecnología** | | **2.2 Software** | **2.2.4.Parámetros de seguridad** |
| **Contexto** | | | | |
| **Descripción** | Una persona externa a la organización mediante la utilización de un malware obtiene credenciales de acceso al sistema y con ellas logra asignar turnos y saturar el sistema. Esto atenta contra la disponibilidad de los turnos | | | |
| **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**: Es altamente afectada. El sanatorio no podrá asignar, dar de baja ni cambiar el estado de los turnos. A su vez, esta saturación trae aparejada la imposibilidad de realizar la admisión afectando todo el proceso. * **Costo de reemplazo**: No es posible reemplazar los turnos * **Sensibilidad**:   + **Reputación:** Se verá afectada debido al malestar que podría ocasionar en los pacientes al no poder atenderse o sacar un turno   + **Ventaja competitiva**: Otros sanatorios podrían hacer uso de la mala prensa recibida   + **Legal / Regulatoria:** El acceso al sistema de turnos dejaría expuesto datos sensibles de los pacientes posibilitando su divulgación por parte del atacante.   + **General**: No aplica * **Volumen:** todos los datos en el sistema de turnos se verán comprometidos.   **Amenazas**   * **Competencia:** en caso de filtración de datos, la competencia podría lanzar una campaña de atracción de pacientes dirigida. * **Internas/Externas:** La amenaza es externa. * **Acción:**    + **Acceso**: Realizada a través de la suplantación de identidad   + **Uso indebido**: Robo de identidad de la persona a la cual se le sustrajeron las credenciales.   + **Divulgación**: El acceso al sistema de turnos dejaría expuesto datos sensibles de los pacientes posibilitando su divulgación por parte del atacante.   + **Modificación**: No aplica   + **Denegación de acceso**: en principio podría considerarse una denegación de acceso con el fin de normalizar el servicio mientras se llevan a cabo las medidas correctivas   **Organización:** El riesgo existe dentro del contexto del sanatorio y el riesgo ocasiona la pérdida de la capacidad de operar normalmente   * **Momento**: La atención sanatorial es continua, aunque tendrá mayor impacto en horario “comercial” donde ocurren la mayor concurrencia de personas para atenciones menores. * **Debido cuidado:** Existen diferentes mecanismos para intentar mantenerse a salvo de este tipo de ataques, pero nunca se puede estar 100% seguro. Estas amenazas están en constante evolución. * **Detección:** La detección es casi inmediata * **Respuesta:** Debido a la constante evolución de este tipo de ataques, se hace muy difícil estar preparado, en consecuencia pueden llevarse a cabo implementaciones de resguardos pero puede no ser suficiente.:   + **Contención**: El personal no está capacitado para afrontar este tipo de problemas.   + **Remediación**: La organización no está preparada para remediar este problema.   + **Recuperación**: La organización no está preparada para remediar este problema.   **Factores externos:**   * **Detección:** Todo el tiempo se están otorgando turnos y el personal tiene conocimientos de la cantidad aproximada de turnos dados posibilitando que cualquier salto brusco en dicha cantidad pueda detectarse con facilidad. * **Legal / Regulatorio**: El acceso al sistema de turnos dejaría expuesto datos sensibles de los pacientes posibilitando su divulgación por parte del atacante. * **Competidores**: en caso de filtración de datos, la competencia podría lanzar una campaña de atracción de pacientes dirigida. * **Medios de comunicación**: De conocerse podría significar mala prensa para el sanatorio. * **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**: se busca instalar un malware con el fin de obtener las credenciales de accesos para poder asignar turnos para así generar una sobreasignación y saturación de los turnos.   **Aleatorio: -- Regular**: **--** **Intencional**: **X**   * **Acción**: Materializada la amenaza de este riesgo el proceso se ve afectado en su operatoria normal.   + **Beneficio**: personales del atacante o de una organización de la competencia. Porque simplemente quiere “divertirse” o practicar sus habilidades como “cracker”. O en otros casos, podría ser de la competencia y querer sacar ventaja obteniendo más pacientes de este sanatorio por lo que busca que el sistema de este no pueda asignar más turnos y que el paciente en vez de ir personalmente elija sacar por la web otro turno en otro lugar.   + **Nivel de esfuerzo**: Bajo. Los empleados no reciben capacitaciones en cuanto a ingeniería social y/o seguridad informática básica.   + **Riesgo de detección**: Alto. Todo el tiempo se están otorgando turnos y el personal tiene conocimientos de la cantidad aproximada de turnos dados posibilitando que cualquier salto brusco en dicha cantidad pueda detectarse con facilidad.   **Vulnerabilidades**: La única posibilidad de resistir las acciones del agente de amenaza es no utilizando el sistema para el registro de los datos que se deben requerir desde una determinada fecha.   * **Capacidad de las amenazas**: requiere conocimientos acerca de la creación y/o manipulación de malware, de controles de acceso y de ingeniería social. * **Capacidad de resistencia**(CR): Bajo. La organización detectará este tipo de amenazas una vez dentro, es decir una vez que el daño ya está hecho. | | | | |
| **Consecuencias** | De no implementar planes de contingencia adecuados, el sanatorio podría incurrir en pérdidas monetarias de gran magnitud, debido al no poder continuar con el proceso de atención médica hasta que se recupere el sistema de turnos.  Además, no debe olvidarse de las posibles consecuencias legales al infringir la ley de protección de datos personales por la divulgación de la información de los pacientes. | | | |
|  |  |  |  |  |

**TRATAMIENTO DE RIESGOS**

| **Id.** 01 | |  | |
| --- | --- | --- | --- |
| **Identificador** | |  | |
| **Especificación** | | Posibilitado por un malware instalado en la máquina de un usuario, una persona externa a la organización logra obtener las claves de acceso de diferentes usuarios y registrar turnos aleatoriamente para diferentes pacientes, generando una sobreasignación y saturación de los turnos | |
| **E S T**  **R A T E G I A S** | **Evitar** | | |
| Por la naturaleza del riesgo y en relación al proceso de asignación de turnos no es posible evitar el riesgo. | | |
| **Transferir** | | |
| Podríamos transferir la asignación de turnos a una empresa tercerizada ante un ataque dirigido como este muy probablemente no consigamos una mitigación real y a su vez deberíamos tener en cuenta nuevos riesgos relacionados a la comunicación con este proveedor. | | |
| **Mitigar** | | |
| Se establecen las siguientes estrategias para mitigar la probabilidad de ocurrencia:   * Instalar y configurar un firewall para los diferentes puntos de entradas a la red de la organización * Instalar y configurar un Sistema de Detección de Intrusos (IDS) y un Sistemas de Prevención de Intrusos (IPS) * Crear e instrumentar el puesto de Administrador de Redes para el monitoreo de las herramientas mencionadas anteriormente. | | |
| **C O N**  **T**  **R**  **O**  **L**  **E**  **S** | Los contarles que garantizan las estrategias de mitigación mencionadas son:  9. CONTROL DE ACCESOS.  9.1 Requisitos de negocio para el control de accesos.  9.1.1 Política de control de accesos  9.4 Control de acceso a sistemas y aplicaciones.  9.4.2 Procedimientos seguros de inicio de sesión  12. SEGURIDAD EN LA OPERATIVA.  12.2 Protección contra código malicioso.  12.2.1 Controles contra el código malicioso.  13. SEGURIDAD EN LAS TELECOMUNICACIONES.  13.1 Gestión de la seguridad en las redes  13.1.1 Controles de red.  13.1.2 Mecanismos de seguridad asociados a servicios en red  16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.  16.1 Gestión de incidentes de seguridad de la información y mejoras.  16.1.3 Notificación de puntos débiles de la seguridad | | |
| **Riesgo Residual** | | | |
| Todos los mecanismos implementados logran reducir la probabilidad de ocurrencia del riesgo. El proceso de asignación de turnos podrá continuar funcionando y al mismo tiempo estamos disminuimos las posibilidades de divulgación de información de pacientes al implementar el doble factor de autenticación.  Aunque no estamos actuando sobre el impacto de este riesgo debido a que una vez accedido al sistemas de turnos, utilizando credenciales válidas le brindaran al atacante el acceso total a la información almacenada allí. | | | |
|  |  |  |  |

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

| **Id.** 01 |  | |
| --- | --- | --- |
| **Identificador** |  | |
| **Especificación** | Posibilitado por un malware instalado en la máquina de un usuario, una persona externa a la organización logra obtener las claves de acceso de diferentes usuarios y registrar turnos aleatoriamente para diferentes pacientes, generando una sobreasignación y saturación de los turnos | |
| **Disparadores** | 1. Imposibilidad de pacientes que llaman para quejarse de la disponibilidad de turnos. 2. Imposibilidad de los empleados de recepción para asignar turnos. 3. Paciente llama para registrar turno y el personal encargado de registrarlo no puede realizar la actividad. 4. Imposibilidad de los empleados de realizar las admisiones de pacientes 5. Imposibilidad de acceder al sistema de turnos. | |
| **Contingencia** | En cualquier caso se debe:   1. Los empleados deben tomar los datos mínimos y necesarios para poder agendar un turno y que el paciente sea informado vía e-mail dándole la libertad de cambiarlo una vez que el sistema se recupere. 2. Informar al área de sistemas y que constate el problema. 3. Admisión de turnos por orden de llegada. Registrar en papel los datos del cliente y administrar todos los papeles que se requieran para el ingreso del paciente. Estos papeles serán guardados en una caja de manera ordenada. | |
| **Recuperación** | El personal de sistemas se encargará de poner en cuarentena el equipo y bajar la carga del sistema de turnos. | |
| **Continuidad de Negocio** | Revisión de la PC afectada para la realización del informe gerencial de la incidencia.  Refuerzo de las reglas del antivirus.  El paciente deberá esperar que el sistema se recupere para poder recibir los estudios realizados o los informes (si se quiere via mail). Si es el informe se realizan dos: uno para que quede registrado en sistema y otro para que se lleve el paciente. | |
| **Controles de Garantía de los Planes** | 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN  Todos los controles de esta categoría.  17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE  LA CONTINUIDAD DEL NEGOCIO.  17.1 Continuidad de la seguridad de la información.  17.1.1 Planificación de la continuidad de la seguridad de la información | |