****

**“LOS RIESGOS INFORMÁTICOS EN LA RED CORPORATIVA”**



**Integrantes:**

**Jocelyn Castañeda Gómez**

**Ricardo Martínez Droguett**

**Jaime Rebolledo Venegas**

**Karen Reyes Silva**

**Loreto Vidal Jerez**

**Rodrigo Vidal Sánchez**

**INTRODUCCION**

Hoy en día el sector salud se está digitalizando cada vez más, los datos utilizados emanan de diferentes sistemas, los cuales se encuentran conectados a internet, transfiriendo información en diferentes plataformas.

Debido a la facilidad de acceso a internet y a equipos informáticos, el ciberespacio es una fuente cada vez más recurrente de amenazas en materia de tecnología de la información de los sistemas de información y sector salud no se encuentra exento de este riesgo, por tal razón, es fundamental que los establecimientos hospitalarios adopten medidas suficientes para establecer una política de ciberseguridad comprensible y robusta que reduzca el impacto de los ciberataques a partir de la prevención y detección temprana.

En presente informe desarrolla el contenido de la vulnerabilidad de los diferentes sistemas utilizados en los diferentes establecimientos hospitalarios públicos, exponiéndolos a eventuales ciberataques o uso malicioso de la información por agentes internos.

Asimismo y con el propósito de entregar una propuesta que permita minimizar los riesgos en esta materia y evitar impactos negativos en la población usuaria del sector interna y externa, se incorporan algunas recomendaciones que podrían ser implementadas en el área de la salud para establecer una política de ciberseguridad.

1. **SISTEMAS DE INFORMACIÓN.**

Al momento de hablar de los sistemas más usados en auditoria, es importante tener en consideración algunos conceptos técnicos que son relevantes en este tema.

FONENDO : Sistema de Registro de prestaciones de Salud

SIRH : Sistema de Información de Recursos Humanos

SIGFE : Sistema de Información para la Gestión Financiera

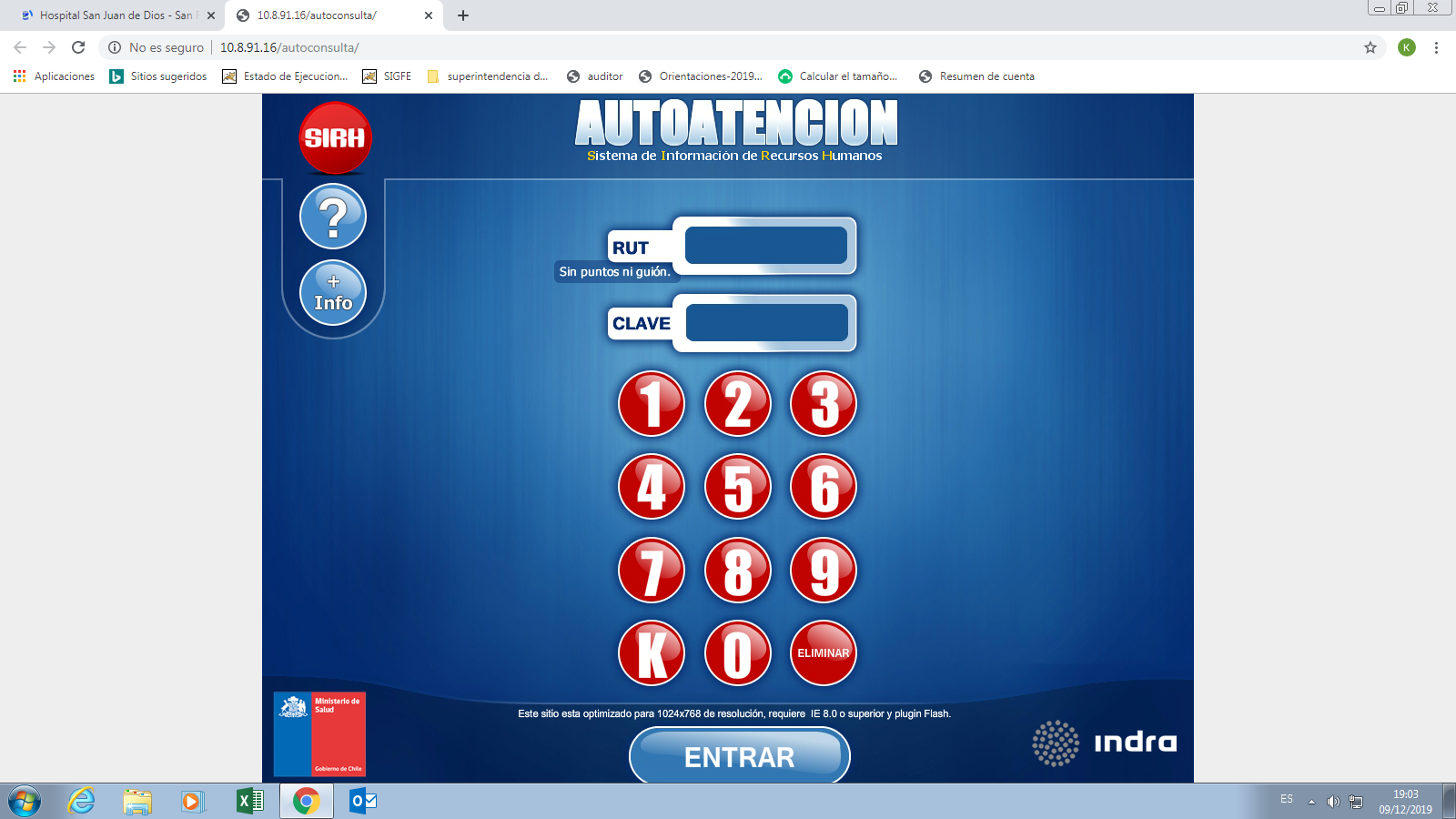
SIGTE : Sistema de Información y Gestión de Tiempos de Espera

REGISTRO CIVIL

GRIFOLS : Sistema utilizado para el despacho de medicamentos en farmacia

RISPAC : Sistema utilizado en Imagenología

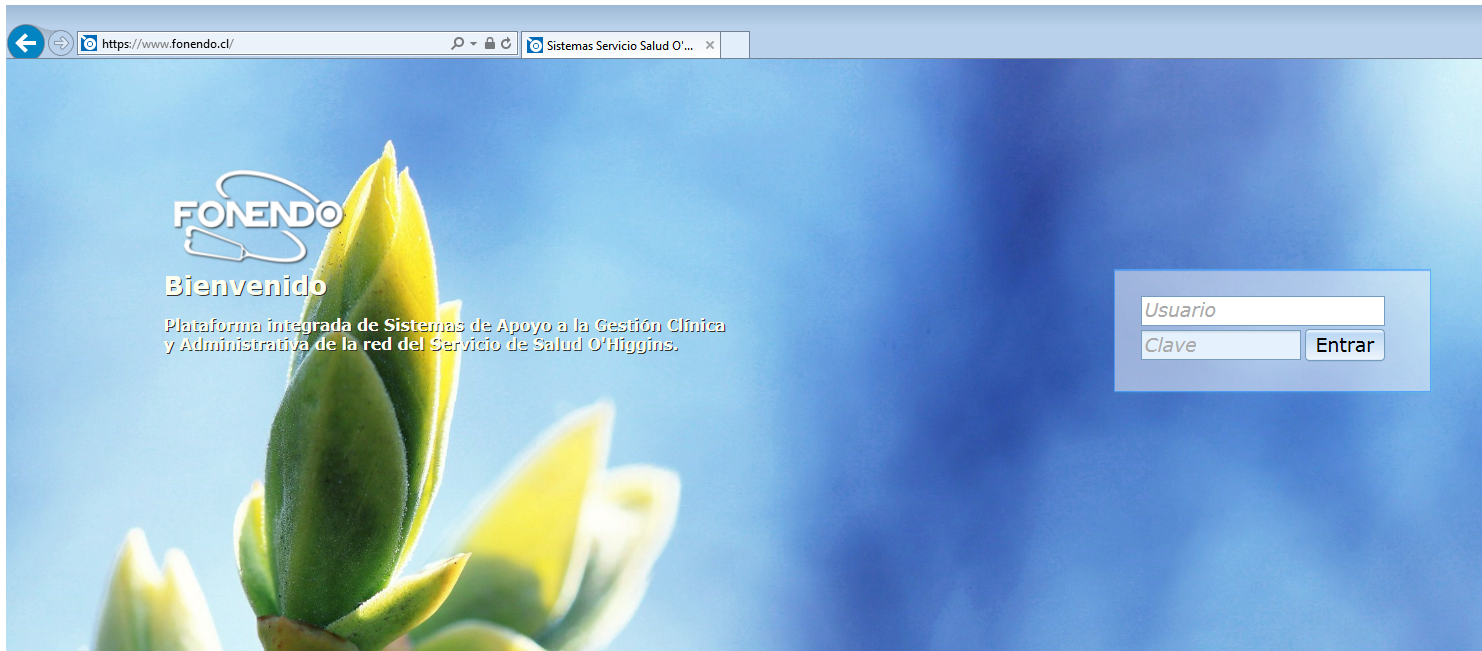
LISPAC : Sistema utilizado en Laboratorio

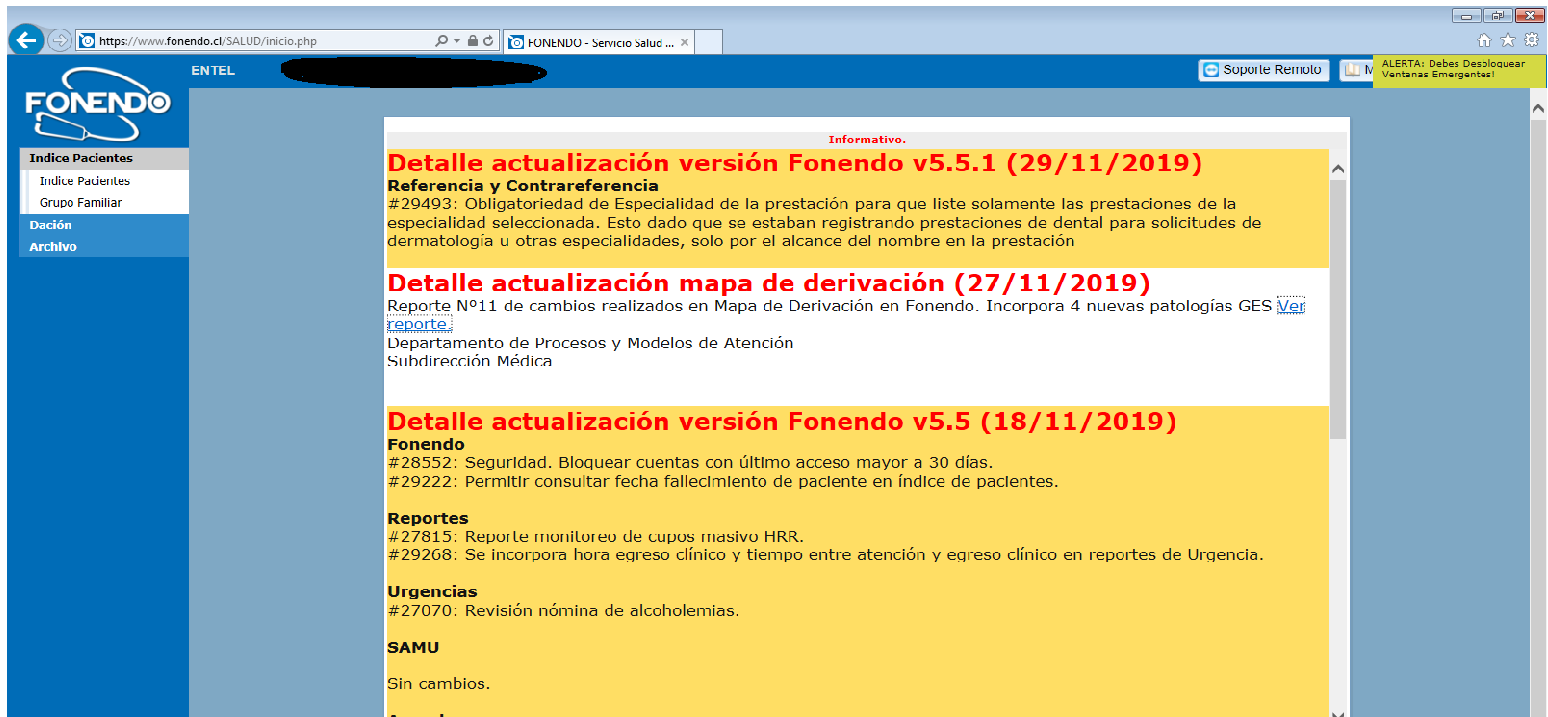


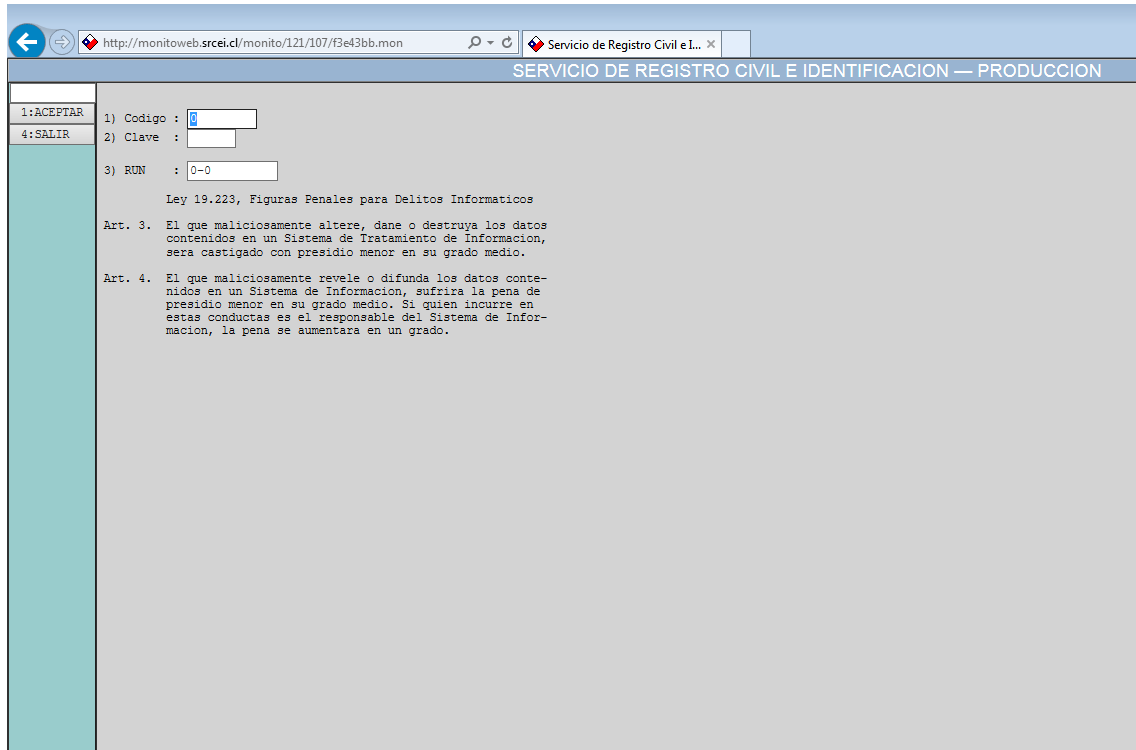












Los activos de información pura de los sistemas a tratar, SIGFE y SIRH, son variados, y van desde los datos digitales como datos personales, financieros, legales y bases de datos.

En los activos intangibles, encontramos datos personales, financieros y legales (sólo en SIRH) y en los intangibles, las relaciones personales (sólo en SIRH). Además encontramos activos físicos, como computadores (en comodato) y activos humanos externos, como soporte.

**SISTEMA DE INFORMACIÓN PARA LA GESTIÓN FINANCIERA DEL ESTADO (SIGFE)**

El Sistema de Información para la Gestión Financiera del Estado (SIGFE), es la plataforma que permite a la DIPRES la captura, procesamiento y exposición de la Ejecución Presupuestaria de todas las instituciones del sector público del Gobierno Central y es concebido como un sistema de información de carácter dinámico, orientado a constituirse en una herramienta de apoyo efectivo para mejorar y dar mayor transparencia a la gestión financiera. Se encuentra operativo todos los días de año bajo una plataforma Web.

El Sistema de Contabilidad funciona en 4 plataformas:

1. SIGFE 1. – Su funcionalidad tiene que ver con la creación de pagos, transferencias, generación de cheques y depósitos.
2. SIGFE 2. – Agrega la conciliación bancaria y transferencias electrónicas
3. SIGFE HOMOLOGADO – Permite que cada Institución tenga su propio sistema contable
4. Las tres reportan a una gran plataforma llamada SIGFE AGREGACIÓN que administran tanto la DIPRES (Dirección de Presupuestos) desde el punto de vista contable, como la Contraloría General de la República en su rol de fiscalizador.

La convivencia entre SIGFE 1 y 2 genera una serie de conflictos de seguridad:

|  |  |
| --- | --- |
| **VULNERABILIDAD** | **AMENAZAS** |
| Validación de datos | Los usuarios que ingresan información al sistema no tienen la obligación de validar su RUT lo que permite crear cuentas con registros erróneos dentro de la información financiera del establecimiento. |
| Registro de datos | No existe un control para verificar si la información se ingresó en horarios y días no hábiles |
| Control de acceso | En caso de SIGFE 2, permite el ingreso de hasta 6 veces la contraseña errónea, seguida de un bloqueo de 10 minutos.  Intento ilimitado de ingresar al perfil del usuario, sin riesgo de bloqueo definitivo. |
| Dualidad de perfiles | Con un mismo usuario se pueden abrir las cuentas en 2 servidores diferentes. |
| Capacidad de demanda al uso de la plataforma | Colapso de plataforma cada fin de mes y fin de año. |

**DE MANERA GENERAL**

**Amenazas**

Acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

Ejemplos.

Malware o códigos maliciosos.

Botnets

Descontrol de redes sociales

Virus

Gusano

Troyano

Keylogger

Spyware

Ransoware

Rootkit

Escaneo de puertos.

**Vulnerabilidades.**

Debilidad en un sistema de información que pone en riesgo la seguridad de la información.

Ejemplos.

Debilidad en el diseño de protocolos utilizados en la red.

Políticas de seguridad deficiente e inexistente

Errores de programación

Configuración inadecuada

Limitación o ausencia de tecnología de la seguridad

Medidas de protección de los sistemas informáticos.

Crear una política de seguridad

Incorporar mecanismos de identificación e autentificación

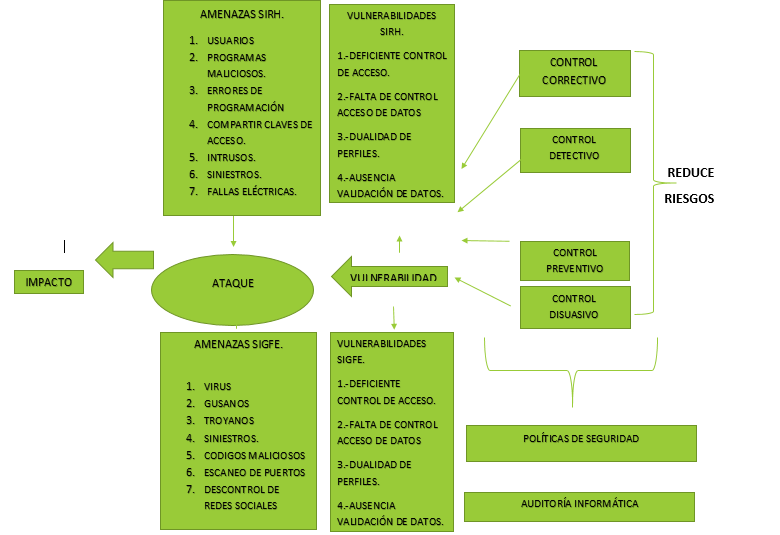
Control de acceso

Incorporar mecanismos de separación (física, temporal, lógica, criptográfica y fragmentación)

Mecanismos de seguridad en las comunicaciones

Ejemplos de programas para efectuar un análisis de vulnerabilidad

Nessus y Conan

****

**CONCLUSIÓN**

Como resultado del tema desarrollado, destacamos la importancia que tiene hoy en día la tecnología de la información en salud, sin embargo la nula interconexión conlleva a errores y la vulnerabilidad del sistema es de un alto riesgo.

Dichos programas en cualquier momento podrían estar expuestos a ataques cibernéticos y ser utilizados de forma maliciosa, provocando un mal funcionamiento o total cese de las funciones lo que provocaría en colapso en la atención y buen funcionamiento de los establecimientos de salud.

Entre los riesgos de la infraestructura crítica se puede señalar que la mayoría de los establecimientos hospitalarios utilizan sistemas de información basadas en plataformas antiguas y con sistemas operativos vulnerables.

Darle la importancia a la ciberseguridad en los hospitales públicos requiere el liderazgo de las autoridades superiores con una política institucional, cambios culturales dentro de la organización y contar con el recurso humano especializado en ciberseguridad, ya que deben actuar como responsables de la seguridad de la información que generan los sistemas, proponiendo y verificando que las medidas de seguridad se aplican correctamente por los responsables técnicos.

Por último, es fundamental que el Estado de Chile y los Hospitales Públicos, implementen medidas de ciberseguridad para mitigar las vulnerabilidades que podrían presentar estos programas, con el propósito de salvaguardar la información tanto de los usuarios internos como externos al servicio de salud.