Confianza, Visión y Resultados

BAKER TILLY CHILE

AUDIT, TAX & CONSULTING

Licitación N° 1260-7-LP12

Auditoría de Procesos TI y Plan de Mejoras de Sistemas Informáticos

Gobierno Regional Metropolitano de Santiago

GUERRA & RABY

an independent member of BAKER TILLY INTERNATIONAL

Santiago, 13 de julio del 2012

Señores
Gobierno Regional Metropolitano de Santiago
Presente

De nuestra consideración:

En base a los requerimientos de la presente licitación, tenemos el agrado de presentar los resultados del Proceso de Auditoría de Procesos TI y Plan de Mejoras de Sistemas Informáticos para el Gobierno Regional Metropolitano de Santiago, en adelante, Gore - RM. El presente informe tiene por objetivo presentar a vuestra consideración el resultado de la evaluación de los sistemas, seguridad informática, y evaluación del departamento de informática, con el fin de presentar el estado de la seguridad de los datos, operación y procesos relacionados.

Lo anteriormente expuesto, se lleva a cabo en cumplimiento a las actividades detalladas en las bases técnicas de la presente licitación, utilizando la Metodología de Exposición al Riesgo, que permite evaluar la severidad de cada riesgo detectado, eficiencia de los controles aplicados para mitigar los mismos, permitiendo conjuntamente otorgar indicaciones al Gore - RM para establecer un plan de protección de la información y los activos, tratando de conseguir la confidencialidad, integridad y disponibilidad de los datos, y las responsabilidades que debe asumir cada uno de los participantes de los procesos y flujos de trabajo de la organización.

Finalmente, como resultado se detallan en el presente informe las debilidades encontradas y se emiten recomendaciones de las mismas, las que contribuirán a mejorar los niveles de seguridad de los procesos y datos del Gore – RM.

Quedamos a su disposición para ampliar y/o aclarar el contenido de las materias tratadas en el presente informe.
Saludamos muy atentamente a ustedes,

Marco Antonio Halal Manzano
Baker Tilly Chile

Contenido

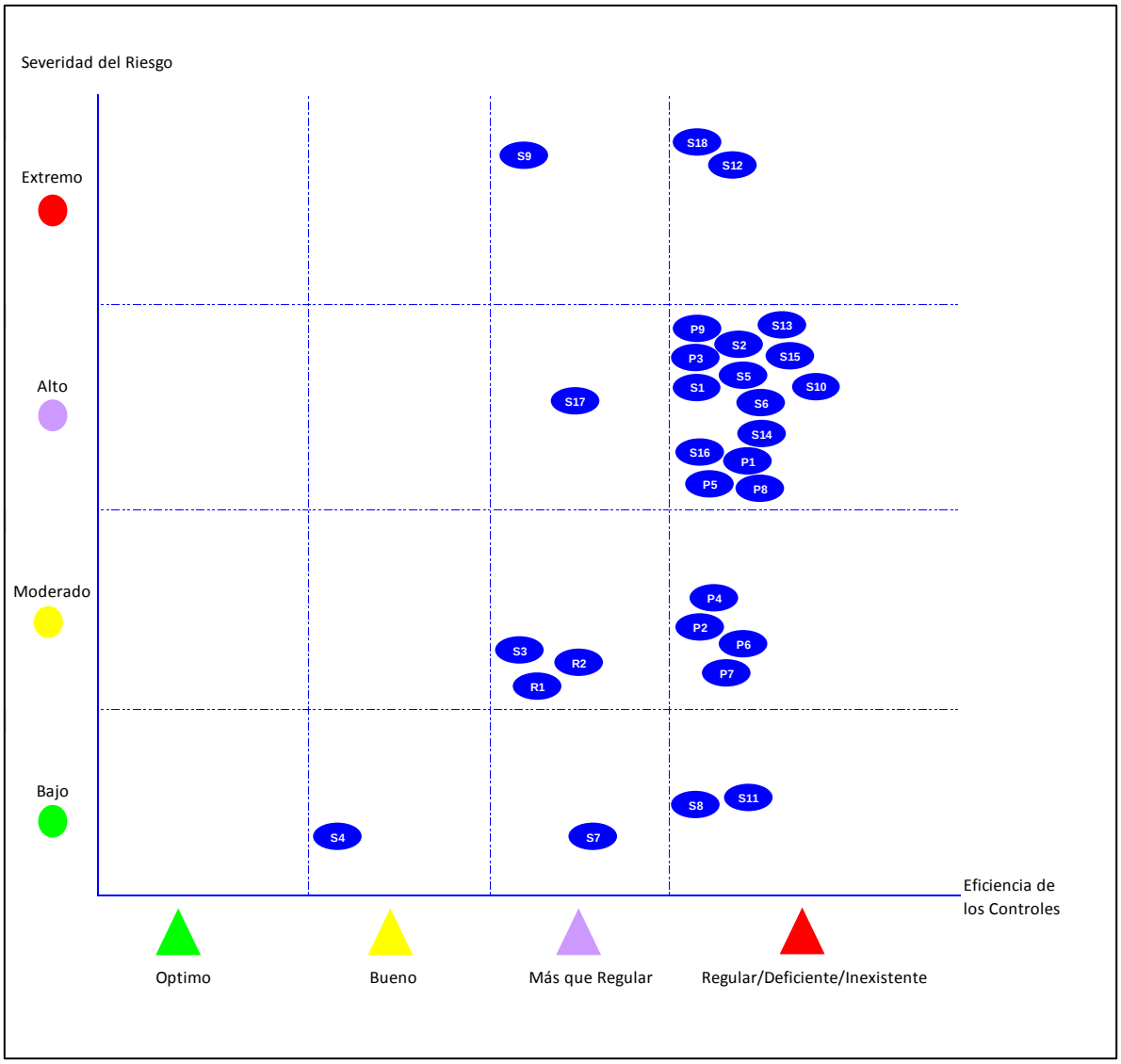
RESUMEN EJECUTIVO

Matriz de riesgos

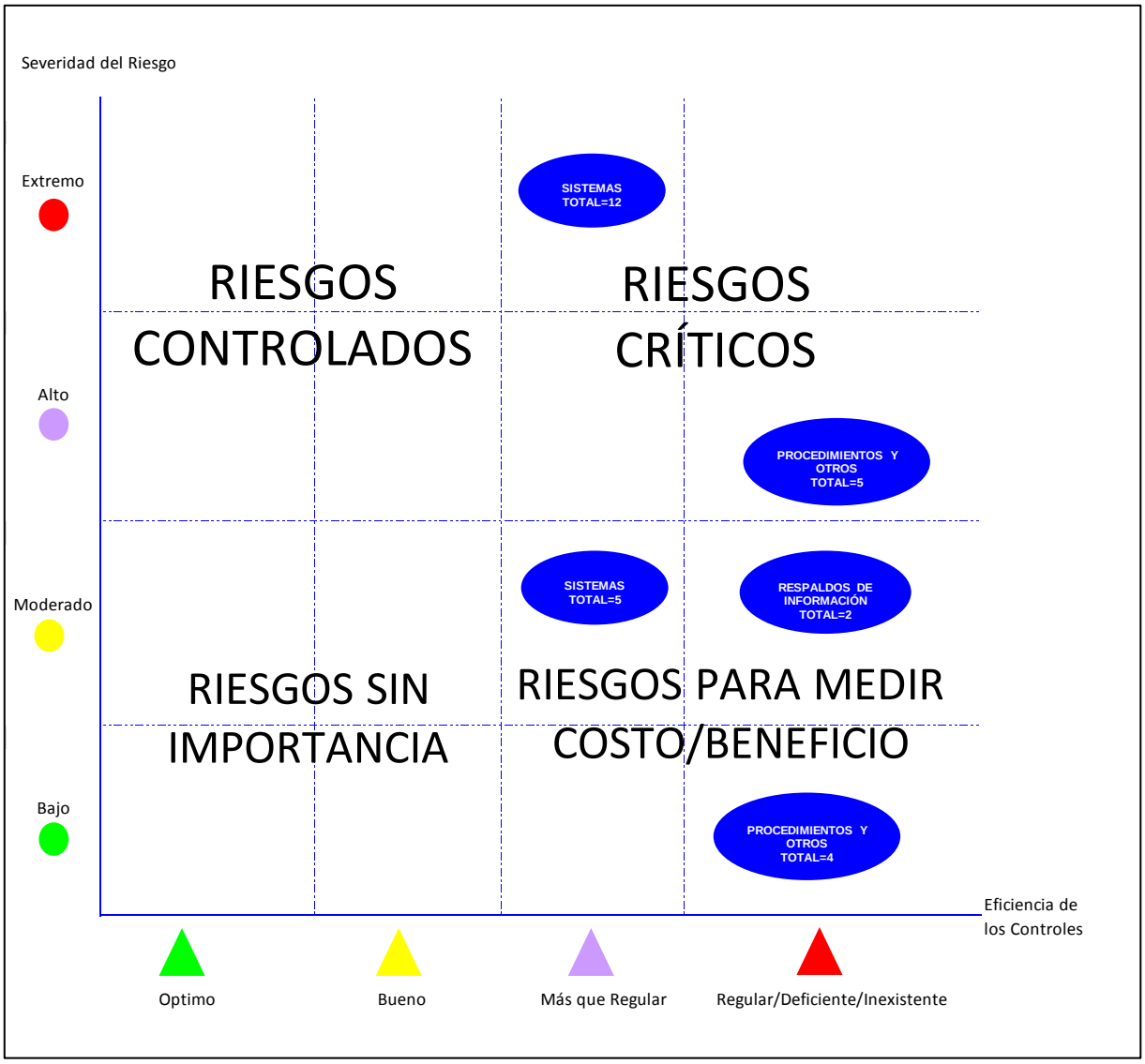
Subproceso	Objetivo del subproceso	Referencia	Severidad del riesgo	Eficiencia de los controles claves	Nivel de exposición al riesgo
			Nivel de Severidad Cualitativa	Clasificación	Clasificación
Evaluación de Sistemas	Evaluación del Cumplimiento de requerimientos de la organización.	S1	Alto	Regular	Mayor
	Evaluación de la seguridad de la comunicación entre los sistemas.	S2	Alto	Regular	Mayor
	Evaluación de la factibilidad y eficiencia de reportes de gestión.	S3	Moderado	Más que regular	Menor
	Evaluación del mantenimiento del equipamiento computacional.	S4	Bajo	Bueno	Menor
	Evaluación de las pruebas de implementación.	S5	Alto	Regular	Mayor
	Evaluación de la documentación de análisis y diseño.	S6	Alto	Regular	Mayor
	Evaluación de la distribución de recursos dentro de la sala de servidores.	S7	Bajo	Más que regular	Menor
	Evaluación del cableado de la sala de servidores.	S8	Bajo	Regular	Menor
	Evaluación de la seguridad en la infraestructura de la sala de servidores.	S9	Extremo	Más que regular	Mayor
	Evaluación del acceso lógico a los servidores.	S10	Alto	Regular	Mayor
	Evaluación del acceso lógico a firewall.	S11	Bajo	Regular	Media
	Evaluación del acceso lógico a los sistemas.	S12	Extremo	Regular	Mayor
	Evaluación del acceso lógico a Portal de Aplicaciones.	S13	Alto	Regular	Mayor
	Evaluación de la seguridad del acceso al Portal de aplicaciones desde internet.	S14	Alto	Regular	Mayor
	Evaluación de la seguridad en el cierre de sesión de los sistemas.	S15	Alto	Regular	Mayor
	Evaluación de la segregación de funciones.	S16	Alto	Regular	Mayor
	Evaluación del perfilamiento de los sistemas.	S17	Alto	Más que regular	Media
	Evaluación de la seguridad en el acceso lógico a la base de datos.	S18	Extremo	Regular	Mayor

Subproceso	Objetivo del subproceso	Referencia	Severidad del riesgo	Eficiencia de los controles claves	Nivel de exposición al riesgo
			Nivel de Severidad Cualitativa	Clasificación	Clasificación
Respaldos de la información	Evaluación del cumplimiento de procedimientos de respaldo de la información.	R1	Moderado	Más que regular	Menor
	Evaluación de la seguridad de los respaldos en dependencias externas.	R2	Moderado	Más que regular	Media
Procedimientos establecidos, cumplimiento y otros factores.	Evaluación del plan de recuperación de ante desastres.	P1	Alto	Regular	Mayor
	Evaluación de los procedimientos de eliminación, reutilización y devolución de activos de información.	P2	Moderado	Regular	Media
	Evaluación de la seguridad de la información en tránsito.	P3	Alto	Regular	Mayor
	Evaluación de la seguridad en la identificación y autenticaciónd e usuarios.	P4	Moderado	Regular	Mayor
	Evaluación del cumplimiento de normativas relacionadas con las contraseñas de acceso.	P5	Alto	Regular	Mayor
	Evaluación de la periodicidad de cambio de las contraseñas de acceso.	P6	Moderado	Regular	Mayor
	Evaluación de la gestión de cuentas genéricas.	P7	Moderado	Regular	Media
	Evaluación de Encargado de Seguridad (Oficial de seguridad).	P8	Alto	Regular	Mayor
	Evaluación de la red institucional.	P9	Alto	Regular	Mayor

Mapa de riesgos



Mapa de riesgos - criticidad



INFORME DE AUDITORIA DE PROCESOS TI Y PLAN DE MEJORAS DE SISTEMAS INFORMATICOS

Capítulo I. Evaluación de Sistemas

Objetivo de auditoría: El equipo auditor evalúa el funcionamiento y desarrollo de los sistemas de información solicitados en la presente licitación, con el fin de recoger, agrupar y evaluar evidencias que permitan determinar si las aplicaciones salvaguardan los activos y mantienen la seguridad de los datos del Gore – RM. Se evalúan además características de los sistemas y controles establecidos para lograr la confidencialidad, integridad y oportunidad de la información procesada.

Durante la presente etapa, se analizó además la documentación asociada a cada sistema, se realizaron entrevistas a los principales usuarios, mediante la aplicación de formularios estandarizados respecto a cada sistema.

I.1. Cumplimiento de requerimientos de la organización

La presente actividad se lleva a cabo principalmente mediante entrevistas con los principales usuarios de los sistemas a evaluar, momento en el cual se aplican formularios estandarizados de acuerdo al funcionamiento y objetivo de cada sistema, principal método para analizar el cumplimiento de los requerimientos de los usuarios.

Por otro lado, se realiza una flujogramación de los procesos, con el fin de evaluar si el ciclo de productivo del Gore – RM se encuentra reflejado claramente en los sistemas evaluados en el proceso de auditoría.

a.- Observación

Durante el proceso de evaluación del cumplimiento de los requerimientos, se pudo observar existen sistemas que no cumplen con los requerimientos de los usuarios, debiendo reemplazar dichas funcionalidades con operaciones manuales complementarias al sistema. A continuación se detallan algunos ejemplos:

- Sistema de Control de Asistencia: En la actualidad el sistema no controla el horario flexible, lo que se debe realizar en forma manual, y conciliar la información al momento de generar informes de asistencia.
- Sistema de Control de Asistencia: El cálculo de atrasos y horas extras se realiza en forma manual, mediante la generación de una planilla en formato .xls (Ms. Excel).

- Sistema de Calificaciones: En caso de error en la calificación, toda modificación debe ser solicitada al Área Informática, quien se encarga de abrir nuevamente la hoja de calificación, modifica lo necesario e informa de la modificación al área respectiva. El sistema no permite a los usuarios realizar las modificaciones requeridas, al menos durante un periodo pre-establecido de tiempo.
- Sistema de Administración y Gestión de la Inversión Regional (SAGIR): El sistema no abarca todo el proceso del negocio, como por ejemplo: Pre-inversión, Proceso Contable.
- Sistema de Administración de Inventario: El sistema no permite a los usuarios realizar modificaciones de los centros de costo, lo cual complica las labores debido a que han ocurrido cambios en el organigrama.
- Portal de aplicaciones: La funcionalidad que permite cambiar la contraseña de acceso, específicamente el botón “Cancelar” no funciona correctamente, al hacer click en cancelar no se realiza ninguna operación.
- Sistema de Preinversión: La funcionalidad que posee el sistema para buscar usuarios no funciona. Al ingresar un dato este buscador no entrega información alguna, incluso con datos de usuarios del sistema.
- Sistema de Preinversión: Al momento de ingresar un nuevo usuario al sistema, el campo “Tipo de Usuario Regional” tiene por defecto “Consejero Regional”, actualmente no permite seleccionar otro tipo de usuario.

Adicionalmente se pudo observar que los usuarios evalúan de manera positiva las decisiones que toma el Comité de informática respecto de las mejoras de los sistemas, así como del Área Informática.

Riesgos y posibles efectos: Se arriesga perdida de la integridad de la información, por errores involuntarios de digitación (eliminación, modificación, ingreso, etc.) que podrían no ser detectados sino hasta el final de los procesos. Además, genera un tiempo adicional evitable en el trabajo del personal asociado a cada sistema.

Nivel de probabilidad de ocurrencia del riesgo: Moderado.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: Con el fin de mitigar los riesgos mencionados anteriormente, se sugiere automatizar los principales procesos.

Comentarios de la administración

Las debilidades comentadas para los Sistemas de Preinversión y de Administración y Gestión de la Inversión Regional (SAGIR), se encuentran levantadas y consideradas dentro del proyecto SAGIR 2.0, el cuál a la fecha se encuentra en etapa de desarrollo y que está programado para su puesta en operación en Enero de 2013.

Lo relacionado con el Portal de Aplicaciones, es una situación ya detectada, que se encuentra considerado en el desarrollo e implementación de la nueva versión del Portal de Aplicaciones que forma parte del Proyecto de Mejora de la Plataforma Tecnológica, el cual se encuentra en su etapa de desarrollo y deberá estar implementado en su totalidad a Diciembre de 2012. Sin embargo lo concerniente al Portal de Aplicaciones se encontrara puesto en marcha durante Agosto del presente año.

Lo relativo a los sistemas de Control de Asistencia, Calificaciones y Administración de Inventarios, serán considerados dentro del Plan Informático 2013, ya que conllevan recursos económicos asociados.

b.- Observación

Se estableció que la comunicación entre los sistemas, para la transmisión y explotación de la información no se realiza de manera automatizada. Actualmente, toda la sincronización de los datos entre los diferentes sistemas se lleva a cabo en forma manual, mediante la carga de archivos planos de un sistema a otro, o la digitación de totales. A continuación, se detallan algunos ejemplos:

- Sistema de Control de Asistencia: No se comunica de manera automatizada con el Sistema de Remuneraciones, toda la información es centralizada mediante la utilización de planillas en formato .xls (Ms. Excel).
- Sistema de Remuneraciones: El sistema no se comunica de manera automatizada con el sistema utilizado por el Contabilidad. La centralización de las remuneraciones se lleva a cabo mediante el envío, vía correo electrónico, de una planilla que contiene las remuneraciones.
- Sistema de Remuneraciones: Se recibe información de descuentos desde el Área de Bienestar para ser almacenada en el sistema (cuota social, préstamos, etc.) e incluirla en el cálculo de la remuneración.

Riesgos y posibles efectos: La no automatización de procesos, o la descentralización de la información es riesgosa, debido a que la intervención constante de los usuarios sobre los datos y procesos mediante diferentes métodos, con el fin de centralizar la información, lo que puede generar errores involuntarios de digitación, pérdida en la integridad de los datos, eliminación

involuntaria, etc., los que pueden no ser detectados sino hasta el final del proceso. Además, se arriesga sobrecarga de labores a los usuarios.

Nivel de probabilidad de ocurrencia del riesgo: Probable.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: A objeto de minimizar los riesgos mencionados anteriormente, se sugiere centralizar la información de los sistemas, mediante transacciones automatizadas de datos de un sistema a otro, así como de un módulo a otro, facilitando con ello la comunicación entre las diferentes áreas de la organización.

Comentarios de la administración

Lo relacionado con la integración del Sistema de Control de Asistencia con Remuneraciones se encuentra en etapa de implementación, por lo que se encontrara en producción en el mes de Septiembre de 2012.

Lo relativo al Sistema de Remuneraciones con el Contabilidad, no podemos realizar modificaciones, ya que el sistema de Contabilidad es el SIGFE, el cuál es centralizado y su única vía de carga de archivos es en formato Excel y en forma manual.

c.- Observación

Algunos sistemas presentan limitantes en los reportes de gestión requeridos por algunas áreas. A continuación, se detallan algunos ejemplos:

- Sistema de Calificaciones: El sistema, en la actualidad permite la generación de reportes de gestión, sin embargo, de acuerdo a lo indicado por los usuarios, éstos son muy básicos, debido a que no emiten puntaje, estado de la evaluación, fecha, estado de notificación, razón por la cual se exporta la información a una planilla en formato .xls (Ms. Excel) y posteriormente se anexan los datos requeridos.
- Sistema de Remuneraciones: Los informes que deben ser enviados a la Dipres, son generados en forma manual, mediante la extracción de datos desde variadas fuentes, debido a que el sistema no permite la extracción directa de dicho reporte.
- Sistema de Administración de Inventario: Este sistema no permite a los usuarios modificar los datos para generar resoluciones (vistas, considerando, etc.), sólo permite modificar la firma y el pie de página, razón por la cual se llevan a cabo en forma manual.

Riesgos y posibles efectos: La situación detectada actualmente podría arriesgar la pérdida de integridad de la información, debido a que se puede incurrir en errores involuntarios durante la digitación, transferencia y trabajo de la información. Además, genera alta dependencia del área a cargo de dicha labor y una sobrecarga de sus labores.

Nivel de probabilidad de ocurrencia del riesgo: Moderado.

Nivel de impacto del riesgo: Menor.

Nivel de severidad del riesgo: Moderado.

Recomendación: Para mitigar los riesgos mencionados anteriormente, se sugiere mejorar las herramientas de gestión de la información proporcionadas por el sistema, adaptándolos a los requerimientos de los usuarios.

Comentarios de la administración

Las observaciones relacionadas con el Sistema de Remuneraciones, son funcionalidades que el actual sistema posee, por lo que realizara una recapacitación de los usuarios, con la finalidad de que se obtenga el mayor provecho de este sistema.

Lo relacionado con los sistemas de Calificaciones y Administración de Inventarios, serán analizados y revisados para ser incorporados en el Plana Anual Informático 2013.

I.2. Mantención, desarrollo de sistemas y equipamiento computacional

Objetivo de auditoría: El equipo auditor evalúa la capacidad del Área de Informática para salvaguardar el correcto funcionamiento de los sistemas, así como la capacidad de satisfacer nuevos requerimientos de los usuarios de los sistemas de información y equipamiento, herramientas fundamentales en el ciclo productivo de la mayoría de las empresas a nivel mundial, tanto públicas como privadas.

I.2.1. Mantención de sistemas

a.- Observación

Durante el proceso de evaluación de los procedimientos de mantenimiento de los sistemas, se pudo observar que el Área de Informática del Gore – RM no presenta problemas en este ítem; el funcionamiento y mejoramiento de los sistemas desarrollados en forma interna, cuentan con un correcto funcionamiento y adecuada capacidad de ser mantenidos.

Riesgos y posibles efectos: No se hallaron debilidades significativas con respecto a este tema.

Comentarios de la administración

I.2.2. Mantención de las estaciones de trabajo y equipamiento computacional

Para que los usuarios puedan desempeñar sus labores de manera adecuada en los sistemas informáticos, es fundamental el correcto funcionamiento del equipamiento computacional asociado. Actualmente, el equipamiento computacional es revisado "On demand", brindando soporte en forma telefónica, remota o in-situ dependiendo del problema.

a.- Observación

Durante el proceso de evaluación de los procedimientos de mantenimiento del equipamiento computacional se pudo observar que no se cuenta con un sistema de gestión de soporte, que permita llevar un control de los problemas más frecuentes, los usuarios con más solicitudes de soporte, medir los tiempos de respuesta, etc.

Riesgos y posibles efectos: Eventual pérdida de control del equipamiento computacional, no pudiendo controlar la cantidad de fallas dentro de un periodo de tiempo, periodicidad de ocurrencia de algunos desperfectos, lo cual impide controlar el buen uso del equipamiento computacional.

Nivel de probabilidad de ocurrencia del riesgo: Poco probable.

Nivel de impacto del riesgo: Menor.

Nivel de severidad del riesgo: Bajo.

Recomendación: Se sugiere implementar un sistema de tickets que apoye las labores de soporte, la toma de decisiones de capacitaciones a usuarios, priorizar mejoras en los sistemas, etc.

Comentarios de la administración

Esta debilidad ya fue detectada y levantada, por lo que en el Presupuesto 2013 del Dpto. de Informática, se considero la adquisición e implementación de una solución de Mesa de ayuda, la cual nos permita implementar un sistema de tickets y poder realizar gestión sobre los mismos.

I.2.3. Desarrollo e implementación de sistemas y equipamiento computacional

Objetivo de auditoría: El equipo auditor evalúa los procedimientos de desarrollo e implementación de software, documentación técnica necesaria, códigos fuente, trazabilidad de las funcionalidades, procedimientos de desarrollo, gestión de calidad implementada, entre otros.

a. Observación

Como resultado del trabajo, se verificó que los usuarios de las diferentes áreas pertenecientes al flujo de trabajo del Gore - RM no participan en las pruebas realizadas a los sistemas.

Riesgos y posibles efectos: Posible incumplimiento a requerimientos reales de los usuarios finales en cuanto a sus sistemas.

Nivel de probabilidad de ocurrencia del riesgo: Probable.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: Se sugiere que durante las pruebas realizadas a las modificaciones de los sistemas, participen activamente los usuarios, con lo que se asegurará el cumplimiento de las necesidades de los usuarios, y que éstas modificaciones o mejoras se ajusten a ellas.

Comentarios de la administración

El presente año con el Análisis, Desarrollo, Documentación e Implementación del Proyecto Mejora de Plataforma Tecnológica, el Dpto., de Informática estableció las directrices para el Levantamiento de Requerimiento y Necesidades, Desarrollo, Implementación, Pruebas Funcionales y Puesta en Marcha de las soluciones desarrolladas internamente en el Servicio.

b.- Observación

Durante la evaluación de los procedimientos, se pudo observar que no se cuenta con documentación de análisis y diseño.

Riesgos y posibles efectos: Existe el riesgo de que el desarrollo de las aplicaciones se vea dificultado en caso de que éste deba ser retomado por personal ajeno al equipo de trabajo. Además, que el desarrollo o modificaciones a las aplicaciones no puedan ser realizados por personal ajeno al equipo de desarrollo actual, o que el tiempo de respuesta no sea el más eficiente.

Cabe recalcar, que se está frente a la posibilidad de pérdida del control de las aplicaciones, incluyendo su desarrollo, el no contar con documentación o una metodología estandarizada a cualquier tipo de desarrollo puede imposibilitar un buen desempeño de los desarrolladores, permitiendo interferir en la toma de decisiones para las mejoras y cambio de requerimientos.

Nivel de probabilidad de ocurrencia del riesgo: Probable.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: Con el fin de mitigar los riesgos mencionados, se sugiere implantar una metodología general de desarrollo, estandarizar la codificación de variables, archivos, etc. con el fin de facilitar el entendimiento del código fuente a personal ajeno al equipo de trabajo en caso de emergencia o remplazo de algún integrante, disminuyendo conjuntamente con ello el tiempo de aprendizaje y adaptación.

Se sugiere además, documentar el análisis, desarrollo de las aplicaciones y cada uno de los cambios de requerimientos realizados.

Comentarios de la administración

El presente año con el Análisis, Desarrollo, Documentación e Implementación del Proyecto Mejora de Plataforma Tecnológica, el Dpto., de Informática estableció las directrices para el Levantamiento de Requerimiento y Necesidades, Desarrollo, Implementación, Pruebas Funcionales y Puesta en Marcha de las soluciones desarrolladas internamente en el Servicio.

I.3. Seguridad Informática – Seguridad Física

Objetivo de auditoría: En este punto se evalúa la seguridad física de la sala de servidores, los equipos, dispositivos, medios de almacenamientos y que estos cumplan con las medidas necesarias en lo relativo a la infraestructura física y al mantenimiento de la seguridad de los recursos del Gore – RM.

I.3.1. Acceso físico a la sala de servidores

Por acceso físico, se entiende a la posibilidad que personal no autorizado pueda tener contacto con los servidores que soportan los sistemas o equipamiento de seguridad relacionado.

a.- Observación

Al evaluar el acceso físico a la sala de servidores, se observa que el Gore – RM cuenta con niveles aceptables de seguridad en el acceso. Se efectúan controles desde la entrada a las dependencias, en se verifica a qué lugar se dirige una persona externa, posteriormente la persona es recibida por la secretaria de informática, cuya puerta tienes acceso mediante tarjeta magnética. Por último, la persona debe circular frente a aproximadamente 5 personas para poder llegar a la puerta de acceso a la sala de servidores, la cual es de material sólido y con acceso mediante tarjeta magnética (sólo el personal autorizado tiene acceso).

Riesgos y posibles efectos: No se encontraron debilidades significativas que comentar.

Comentarios de la administración

I.3.2. Distribución de los recursos en la sala de servidores

La sala se servidores cuenta con la adecuada distribución del equipamiento que está en su interior y una correcta aislación del resto de las dependencias, al no presentar ventanas ni múltiples accesos.

a.- Observación

Sin perjuicio de lo anterior, existe equipamiento ubicado en el suelo (servidores), los cuales no son del tipo “rackeable”.

Riesgos y posibles efectos: Se arriesga daños involuntarios en el equipamiento, debido a que los trabajadores que cuentan con acceso pueden tropezar con el equipamiento al desplazarse por la sala, amenazando con ello además la integridad del personal.

Nivel de probabilidad de ocurrencia del riesgo: Muy poco probable.

Nivel de impacto del riesgo: Menor.

Nivel de severidad del riesgo: Bajo.

Recomendación: Se propone mejorar la ubicación del equipamiento.

Comentarios de la administración

Esta debilidad ya fue detectada y levantada, por lo que en el Presupuesto 2013 del Dpto. de Informática, se considero actualización de la Plataforma de Servidores, incluyéndose en los Proyectos de Virtualización y de Implementación de un Site de Contingencia.

b.- Observación

No todos los cables están rotulados en forma adecuada.

Riesgos y posibles efectos: Se arriesga tiempo de respuesta excesivo a la hora de realizar cambios de máquinas, mantenimiento de las mismas o desconexiones involuntarias de equipamiento por parte del personal de mantenimiento y soporte.

Nivel de probabilidad de ocurrencia del riesgo: Muy poco probable.

Nivel de impacto del riesgo: Menor.

Nivel de severidad del riesgo: Bajo.

Recomendación: Se sugiere rotular el cableado del equipamiento perteneciente a la sala de servidores.

Comentarios de la administración

Se tomarán las acciones necesarias para la normalización en el Rotulación del Cableado, el cuál se encontrara finalizado en el mes de Octubre de 2012.

I.3.3. Seguridad en la infraestructura de la sala de servidores

a.- Observación

Por motivos desconocidos, en la sala de servidores existe una tubería de agua, que contiene una llave que funciona correctamente. Según comentarios de personal del Área Informática, al girar la llave, sale agua de ella sin ningún problema (por motivos de seguridad el equipo auditor no giro la llave como prueba).

Riesgos y posibles efectos: Se arriesga daños en el equipamiento, o pérdida total de los mismos, así como también de la información que estos almacenan. Por otro lado, dicha situación puede afectar la disponibilidad de los servicios en caso de daños de maquinaria.

Nivel de probabilidad de ocurrencia del riesgo: Moderado.

Nivel de impacto del riesgo: Mayor.

Nivel de severidad del riesgo: Extremo.

Recomendación: Para mitigar los riesgos mencionadas, se sugiere la eliminación o bloqueo permanente del paso de agua desde el origen, no basta con sólo tapar permanentemente el fin de la cañería, dado que esta se podría reventar frente a fuertes presiones del agua, terremotos, etc.

Comentarios de la administración

Se realizara la coordinación con el Depto. de Servicios Generales con la finalidad de dar una solución Urgente a esta situación.

I.4. Seguridad Informática - Seguridad Lógica

Objetivo de auditoría: Se evalúa los controles de accesos a los sistemas y a los datos que estos gestionan, con el fin de señalar irregularidades que obstaculicen la confidencialidad, exactitud y disponibilidad de la información, y las mejoras que fueran factibles de ser realizadas.

1.4.1. Acceso lógico a servidores.

El acceso lógico se enfoca principalmente en los niveles de seguridad que presentan los servidores y sistemas para sus accesos de software.

a.- Observación

El servidor de preinversión (200.75.2.51) presenta un servicio de base de datos mysql visible desde internet, aunque se encuentra protegido por usuario y contraseña, un atacante podría utilizar ataques de fuerza bruta, como por ejemplo probar accediendo con claves “111”, si esta no funciona “112”, mediante procesos automatizados, hasta lograr acceso a este servicio.

Riesgos y posibles efectos: Se arriesga acceso desautorizado a información confidencial, la filtración y divulgación de los mismos.

Nivel de probabilidad de ocurrencia del riesgo: Poco probable.

Nivel de impacto del riesgo: Mayor.

Nivel de severidad del riesgo: Alto.

Recomendación: En base a las buenas prácticas de la industria, se sugiere cerrar el acceso desde internet y configurar esta entrada sólo a las ip que corresponda.

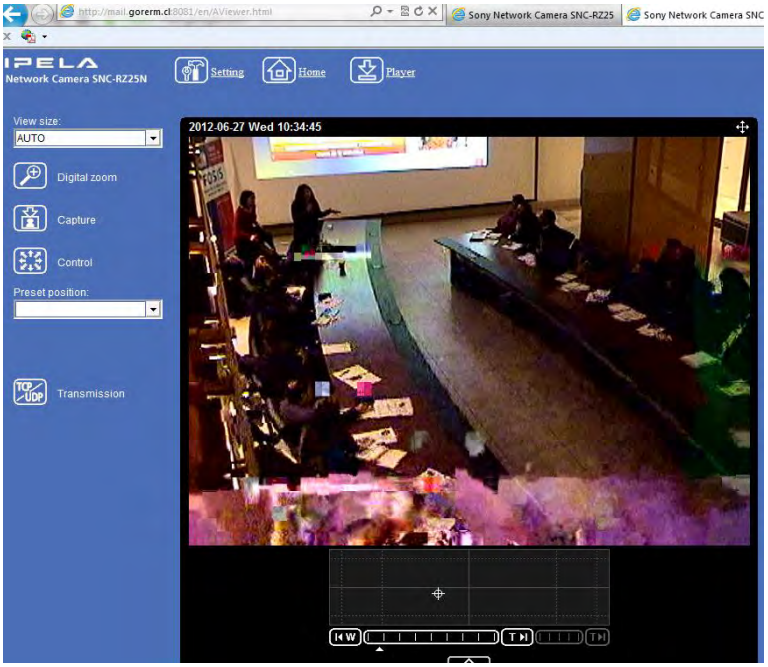
Comentarios de la administración

Las debilidades comentadas para los Sistemas de Preinversión, se encuentran levantadas y consideradas dentro del proyecto SAGIR 2.0.

De igual forma se realizará en forma inmediata el bloqueo del acceso a la base de datos mencionada.

b.- Observación

En el acceso lógico al Firewall 2da capa GORERM (200.75.2.62), se pudo observar, el día 27 de junio del presente año, el funcionamiento de cámaras web de alguna de las salas de reuniones del Gore – RM, personal participante de la reunión, mediante el manejo del zoom de las cámaras, etc. Además, fue posible girar las cámaras sin mayor problema. A continuación, de presentan imágenes detallando lo detectado.



Riesgos y posibles efectos: Se arriesga pérdida de confidencialidad en reuniones realizadas.

Nivel de probabilidad de ocurrencia del riesgo: Poco probable.

Nivel de impacto del riesgo: Menor.

Nivel de severidad del riesgo: Bajo.

Recomendación: La situación mencionada anteriormente no fue constante en el tiempo, por lo que el equipo auditor estima que se trataba de pruebas de dichas cámaras, sin embargo, con el fin de minimizar los riesgos, se sugiere realizar pruebas de este tipo sobre servidores o equipos del área informática que no cuenten con conexión directa desde internet.

Comentarios de la administración

El acceso a este servidor, se encontraba abierto ya que se estaban realizando las pruebas de funcionamiento con la empresa proveedora, con el objetivo de verificar la calidad y el tiempo de desfase en su acceso vía Internet.

1.4.2. Acceso lógico a los sistemas

El acceso lógico a los sistemas se enfoca principalmente en los niveles de seguridad en el ingreso a los sistemas a ser evaluados en la presente auditoría.

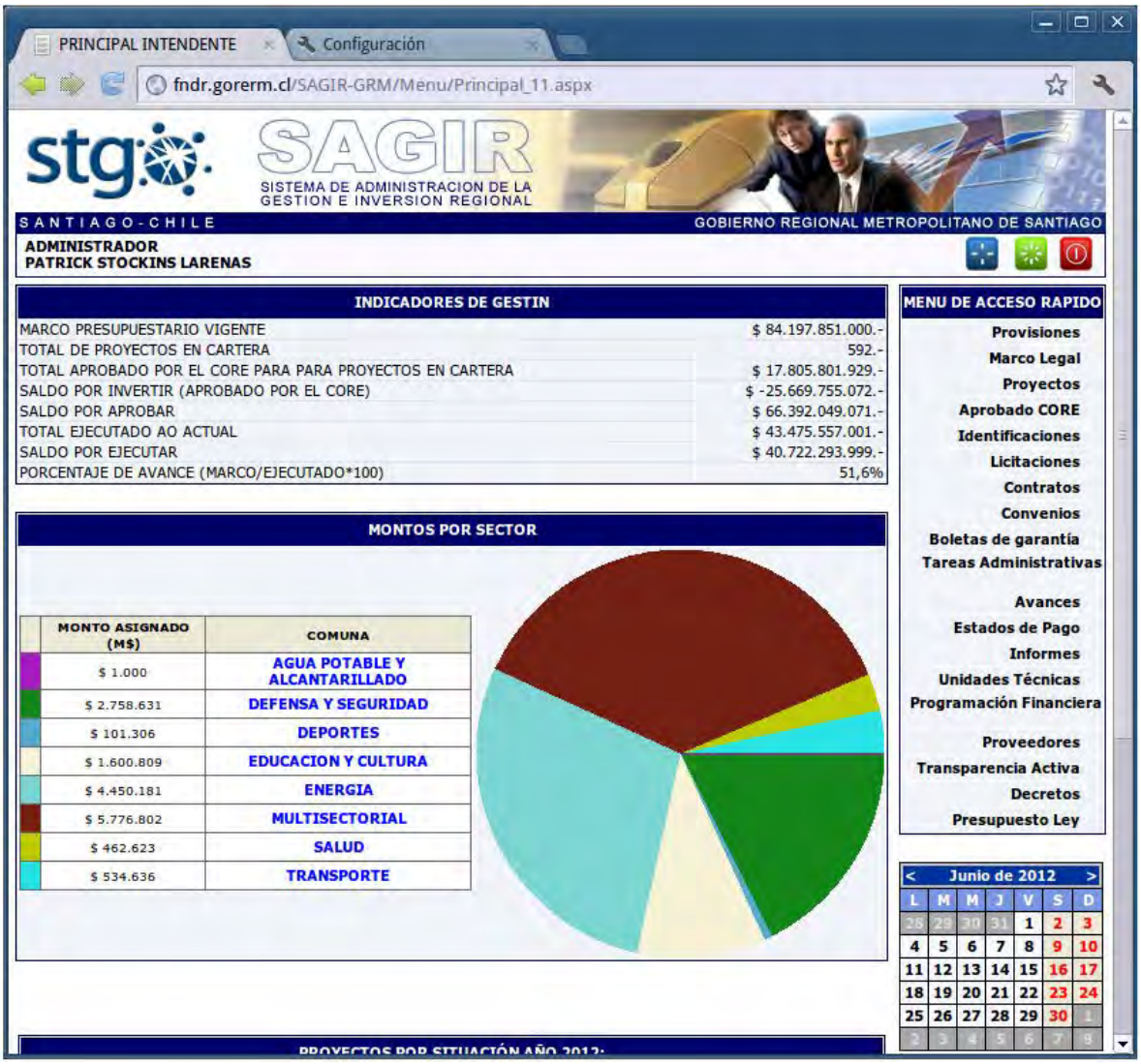
a.- Observación

Durante el proceso de evaluación del acceso lógico a los sistemas, se pudo observar que el ingreso al portal de aplicaciones es vulnerable a inyección de SQL. Una inyección SQL se produce cuando un atacante introduce código de sentencias SQL para realizar acciones como obtener, modificar o eliminar información de las bases de datos, a los cuales no tendría acceso en condiciones normales.

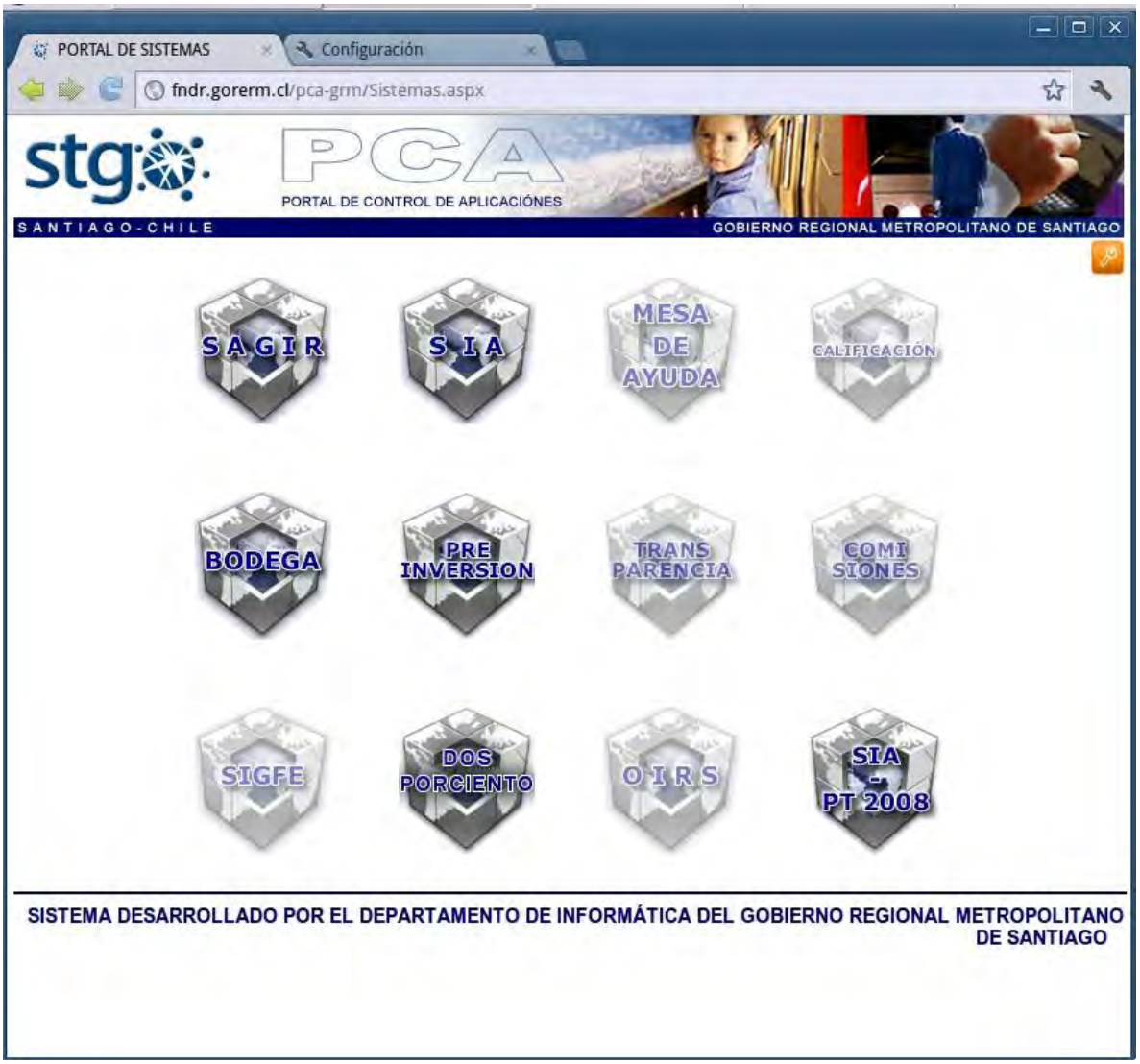
En el Portal de Aplicaciones del Gore - RM (http://fndr.gorerm.cl/PCA-GRM/login.aspx) se solicitan los datos rut y clave. Para un atacante externo, primero debería tener conocimiento del nombre de algún trabajador del Gore - RM, a lo que puede tener acceso utilizando Google (u otro buscador) y por ley de transparencia es posible acceder al listado de trabajadores. Posteriormente utilizando un buscador (Google) es posible acceder a documentos como contratos, actas, etc. en los cuales se pude encontrar el rut de los trabajadores.

Por ejemplo, en el documento "Servicio de desratización, desinsectación y sanitización para las dependencias del Gobierno Regional Metropolitano y Parque Lo Errázuriz" (http://www.gobiernosantiago.cl/Transparencia/ARCHIVOS/549-11.pdf), se obtiene el rut 10.824.825-4, del señor Patrick Stockins Larenas, Jefe de la División de Administración y Finanzas. Una vez que el equipo auditor contó con este dato, se procedió a inyectar una sentencia básica de SQL, ingresando en la contraseña 'or 'x'='x, lo que genera que un atacante se salte la verificación de la contraseña e ingrese como un usuario autentificado, pudiendo elegir a que sistema acceder (siempre y cuando el usuario original tenga los permisos necesarios). Este proceso fue repetido con varios rut de los trabajadores del Gore – RM, dentro de los cuales se pueden mencionar: Viviana Grandon, Pablo Torrealba, Rosa Elena Veliz, Patricio Osorio Zúñiga, Nelson Drago Miranda,

Luis Muñoz Muños, entre otros. A continuación, se pueden observar imágenes que detallan lo mencionado anteriormente.



En la siguiente imagen se presentan las opciones que posee el señor H.Salinas.



Riesgos y posibles efectos: Acceso desautorizado a la información, así como filtración y divulgación de la misma.

Nivel de probabilidad de ocurrencia del riesgo: Probable.

Nivel de impacto del riesgo: Mayor.

Nivel de severidad del riesgo: Extremo.

Recomendación: Con el fin de minimizar los riesgos mencionados anteriormente, se sugiere realizar la modificación necesaria para evitar que se puedan inyectar sentencias SQL en cualquier

parte de los sistemas, en especial en los procesos de autentificación. Es altamente recomendable mejorar la seguridad en el desarrollo de los sistemas.

Comentarios de la administración

Las debilidades detectadas en el Portal de Aplicaciones, es una situación ya detectada, que se encuentra considerada en el desarrollo e implementación de la nueva versión del Portal de Aplicaciones el cual será puesto en marcha durante Agosto del presente año.

La nueva versión del Portal de Aplicaciones no permitirá el ingreso de inyecciones SQL en forma directa en ninguna parte de la plataforma.

b.- Observación

Durante el proceso de evaluación del acceso lógico a los sistemas, se pudo observar que el Portal de Aplicaciones no bloquea los intentos de ingreso, tras varios ingresos de contraseña o usuario erróneos. Un malicioso podría intentar ingresando varios rut (de trabajadores de la institución, ver punto anterior) y claves diferentes, hasta obtener la combinación correcta (ataques de fuerza bruta).

Riesgos y posibles efectos: Acceso desautorizado a la información, también filtración y divulgación de la misma.

Nivel de probabilidad de ocurrencia del riesgo: Moderado.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: Con el fin de mitigar los riesgos mencionados anteriormente, se recomienda realizar un proceso de bloqueo por ip en el servidor y no en el cliente, ya que existen sistemas que realizan bloqueos de intentos fallidos dejando cookies en los clientes, lo cual es fácil de eludir.

Comentarios de la administración

En el desarrollo del nuevo Portal de Aplicaciones, se encuentra considerada la implementación del bloqueo de la IP en el servidor posterior a los 3 intentos, debiendo posterior a esto solicitar al Depto. de Informática el desbloqueo de la dirección IP.

c.- Observación

El Portal de Aplicaciones es accesible desde internet. Un atacante podría, desde cualquier parte del mundo, tratar de ingresar a los sistemas utilizando las técnicas mencionadas anteriormente.

Riesgos y posibles efectos: Se arriesga acceso desautorizado a la información, así como también filtración y divulgación de la misma.

Nivel de probabilidad de ocurrencia del riesgo: Moderado.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: Para mitigar estos riesgos, se sugiere analizar la necesidad de obtener acceso desde internet a las aplicaciones versus el riesgo que esto representa, en caso de que "algunos" usuarios del Gore - RM realmente necesiten tener acceso desde dependencias externas. Es recomendable establecer una red privada virtual y desde ahí tener acceso a los sistemas.

Comentarios de la administración

En la actualidad se permite el acceso a esta plataforma desde Internet, ya que en algunos casos los usuarios realizan trabajos en sus hogares o los fines de semana. Sin embargo se habilitara un Certificado Digital para este sitio con el objetivo de minimizar este riesgo.

d.- Observación

El Portal de Aplicaciones no cierra la sesión definitivamente. En la actualidad, cuando un usuario cierra la sesión, y selecciona "Retroceder página" en el navegador, la sesión vuelve a ser iniciada, sin necesidad de solicitar ingreso de usuario y contraseña nuevamente.

Riesgos y posibles efectos: Filtración de información confidencial, y pérdida de integridad de los datos.

Nivel de probabilidad de ocurrencia del riesgo: Moderado.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: Para minimizar los riesgos, se recomienda mejorar los niveles de seguridad en el código fuente para el correcto cierre de sesión del sistema.

Comentarios de la administración

En la actualidad se permite el acceso a esta plataforma desde Internet, ya que en algunos casos los usuarios realizan trabajos en sus hogares o los fines de semana. Sin embargo se habilitara un Certificado Digital para este sitio con el objetivo de minimizar este riesgo.

e.- Observación

Existen usuarios que tienen acceso a aplicaciones y funcionalidades que no necesariamente les corresponde de acuerdo a las tareas asignadas a su cargo, como por ejemplo, Patricio Osorio Zúñiga, quien es Jefe del Área de RRHH y tiene acceso a SIA (Plan de compras, Proveedores, etc.).

Riesgos y posibles efectos: Acceso a información a la cual no deben tener acceso, aumentando las probabilidades de filtración de datos, errores o pérdida de integridad en la información.

Nivel de probabilidad de ocurrencia del riesgo: Moderado.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: Se sugiere evaluar el listado de usuarios por cada sistema con sus atribuciones, limitando los permisos a las funciones de cada persona.

Comentarios de la administración

Se realizara el análisis correspondiente entre los usuarios existentes y los diferentes privilegios y accesos a los sistemas.

f.- Observación

Los usuarios del Sistema de Administración y Gestión de la Inversión Regional (SAGIR) no se manejan perfilados. Los analistas tienen todas las atribuciones, si borran un contrato y este tiene asociada una boleta, esta queda no asignada.

Riesgos y posibles efectos: Acceso a información a la cual no se debe tener, aumentando las probabilidades de filtración de datos o pérdida en integridad de la información.

Nivel de probabilidad de ocurrencia del riesgo: Moderado.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: Se sugiere realizar perfilamiento de los usuarios de todos los sistemas.

Comentarios de la administración

Esta sugerencia se encuentra levantada y es parte del Proyecto SAGIR 2.0, el cual se encuentra en desarrollo.

g.- Observación

Es posible obtener información del sistema administrador de base de datos. Mediante técnicas de inyección de SQL en conjunto con software "libre" especializado y, dado que no hay una protección adecuada, es posible obtener información sensible del sistema administrador de base de datos, en el caso estudiado en profundidad se logró listar las bases de datos contenidas en el servidor, algún atacante malicioso "podría" modificar, eliminar o acceder a la información contenida.

Es importante destacar que, dado el tiempo contemplado en este trabajo, no fue posible revisar todas las posibilidades de inyección SQL de todos los sistemas, ya que es una tarea lenta y con muchos campos que se podrían probar. Por otra parte, el equipo auditor no realizó ninguna operación que comprometiera la integridad, confidencialidad o disponibilidad de la información.

Se violentó la variable cod de la url:

http://fndr.gorerm.cl/SAGIR-GRM/Proyectos/Ficha_Imprimir.aspx?cod=123

Se obtuvieron las siguientes bases de datos (excluyendo las propias del sistema):

ABOGADOS, ACTIVOF, ADMENTOR, ADMINISTRATIVO2, ADQUISICIONES, BODEGA, CDC, CDC1, CMS, CMS2, COMUN, COMUN_USUARIOS, EDCV4, ESTADISTICAS_REGIONALES, FDA, HELPDESK2, IFRAMES, INTERFAZ_SIGFE, LOG_SISTEMAS, MATRIX, OFICINA_PARTES, OIRS, PCA, PREINVERSION, REM_GORE, RENTA_RRHH, RETIRO, ReportServer, ReportServerTempDB, SAGIR, SAGIR2, SAGIR_2.0, SAGIR_CONSULTA, SEC, SGA, SGD2, SGD2_PRUEBAS, SIA, SIGNER, SIS, TESTER, TRANSACCIONES, TRANSPARENCIA, WS_GORE, ZETAHELPDESK, adq, funcionarios_anexos, intranetRRHH, inv, master, model, msdb, personas, pyr, pyrTEST, seguridad, tempdb.

Riesgos y posibles efectos: Acceso desautorizado a la información, filtración y divulgación de la misma.

Nivel de probabilidad de ocurrencia del riesgo: Probable.

Nivel de impacto del riesgo: Mayor.

Nivel de severidad del riesgo: Extremo.

Recomendación: A fin de minimizar los riesgos mencionados anteriormente, se sugiere realizar la modificación necesaria para evitar que se puedan inyectar sentencias SQL a todos los sistemas, no

basta sólo con poner una validación de longitud de campo corta, o cualquier otra validación “en el lado del cliente, ya que son fáciles de eludir.

Comentarios de la administración

Dentro del Proyecto de Modernización de la Plataforma Tecnología, se encuentra considerado la modificación de los sistemas existentes para que se no permita el ingreso de inyecciones SQL en forma directa en ninguna parte de la plataforma.

Así mismo este requerimiento es parte de los desarrollos de las nuevas soluciones que forman parte de este proyecto.

Capitulo II. Respaldos de la información

Objetivo de auditoría: El equipo auditor evalúa los procedimientos y políticas de resguardo de la información almacenada en las estaciones de trabajo y servidores del Gore - RM, aplicados por el Área de Informática, con el fin de resguardar la información de gestión relacionada con los sistemas.

Los respaldos son fundamentales en toda organización, en ellos se contienen los datos históricos necesarios para restablecer información en caso de contingencias, pérdidas o modificaciones involuntarias. En la actualidad, en el Gore - RM, esta tarea se encuentra dividida en dos acciones, el respaldo de los sistemas y datos de usuarios, por parte del encargado de respaldos y, el depósito de estos respaldos en dependencias externas, utilizando medios magnéticos (cintas).

II.1. Respaldos de Sistemas y de Datos de usuario.

El encargado de respaldos se ocupa de realizar el backup de sistemas y datos de usuarios, para esto, el Área de Informática cuenta con procedimientos que indican cómo y cuándo se realizarán los respaldos.

a.- Observación

Los procedimientos de respaldo de la información no se cumplen a cabalidad, debido a que no se realizan con la frecuencia establecida, cuando la persona responsable de ellos no se encuentra disponible, ya sea por salud, vacaciones, etc. Así mismo, en los procedimientos no se establece la necesidad de una bitácora de los respaldos, en el cual, el encargado de los mismos indique los detalles más importantes de este proceso, como fecha y hora de inicio-termino, información respaldada, medio en el cual está el respaldo y la firma del jefe de informática para cada punto.

Riesgos y posibles efectos: Pérdida del control de los respaldos y la posibilidad de que éstos no funcionen correctamente en caso de requerir restauración de datos por contingencia.

Nivel de probabilidad de ocurrencia del riesgo: Improbable.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Moderado.

Recomendación: A objeto de disminuir los riesgos mencionados, se sugiere modificar y controlar el cumplimiento del procedimiento de respaldos, indicando la generación de una bitácora y detallar el personal alternativo que realice las acciones de respaldos en caso de ausencia del encargado titular.

Comentarios de la administración

Se realizaran las revisiones de los procedimientos actuales, con el objetivo de realizar las actualizaciones y mejoras necesarias para solucionar estas debilidades.

II.2. Resguardo de respaldos en dependencias externas.

En la actualidad, el Gore - RM cuenta con un servicio de resguardo de respaldos en medios magnéticos con la empresa Pipax. El equipo auditor realizó una visita a las dependencias, en compañía del encargado de respaldos, ocasión en la que se pudo observar que la empresa cuenta con medidas de seguridad y procedimientos asociados acordes a los requerimientos de este tipo de servicios.

a.- Observación

Existe falta de rigurosidad en el proceso de respaldos que se almacenan al exterior del Gore – RM. Actualmente, los resguardos externos se realizan "on demand", no se respeta la periodicidad establecida en la norma interna de respaldo.

Riesgos y posibles efectos: Pérdida de respaldos históricos.

Nivel de probabilidad de ocurrencia del riesgo: Poco probable.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Moderado.

Recomendación: Es vital respetar los plazos establecidos en el procedimiento (semanalmente), para el "depósito" de respaldos en las dependencias externas. Adicionalmente, mantener una bitácora propia (no sólo la que se lleva en Pipax), en donde se especifique que fue respaldado, fecha y hora de salida, firmas del encargado de respaldos (o su subrogante) y la del jefe del área informática.

Comentarios de la administración

Se realizaran las revisiones de los procedimientos actuales, con el objetivo de realizar las actualizaciones y mejoras necesarias para solucionar estas debilidades.

Capitulo III. Cumplimiento de Procedimientos establecidos y otros factores

III.1. Plan de prevención y recuperación ante desastres

En la actualidad, se cuenta con un documento denominado "Instructivo de Contingencia", sin embargo, este se enfoca principalmente en documentar los incidentes más que en desarrollar un plan que permita afrontar distintos tipos de contingencias, en la menor cantidad de tiempo y costos asociados.

a.- Observación

El actual plan no cubre las expectativas y objetivos que se busca con este tipo de documentos. El sólo hecho de documentar y tratar de aprender de los incidentes no es suficiente para instituciones de la envergadura del Gore – RM, dado que los acontecimientos que podrían afectar el correcto funcionamiento informático de la institución serán siempre mayores a las experiencias documentadas, por lo que se debe estar preparado para cualquier tipo de eventualidades.

Riesgos y posibles efectos: Que el personal no esté en condiciones de responder en forma oportuna y eficiente en caso de contingencias o desastres, retardando de manera considerable el tiempo de volver a las labores normales, con los consiguientes costos evitables.

Nivel de probabilidad de ocurrencia del riesgo: Probable.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: Con el fin de minimizar los riesgos mencionados anteriormente, se recomienda la implementación y desarrollo de un Plan de prevención y recuperación ante desastres (PRD), debidamente detallado y formalizado. Es aconsejable mejorar y completar este documento siguiendo la siguiente pauta:

1. Establecimiento del escenario a recuperar. (Enumerar cada escenario, desde caídas de servicio, hasta acontecimientos que impidan el usar dependencias habituales de la institución como el caso de Terremotos, etc.).
2. Definición de los tipos de operación en una contingencia.
3. Establecimiento de las criticidades:
    a. Por equipos.
    b. Por servicios.
    c. Por Aplicaciones.

4. Determinación de las prestaciones mínimas.
5. Análisis de Riesgos:
    a. Probabilidad de ocurrencia de desastres.
    b. Determinación de los niveles de desastres.
6. Presentación de las distintas estrategias posibles de recuperación.
7. Selección de la estrategia de recuperación.
8. Elaboración de la estrategia de recuperación adecuada a la institución.
9. Mitigación de Riesgos.
10. Descripción de la estrategia.
11. Requerimientos para llevar a cabo el plan.
12. Esquemas técnicos con los pasos a seguir.
13. Formación del equipo de recuperación del entorno ante desastres (ERED):
    a. Asignación de roles y responsabilidades.
    b. Establecimiento de los procedimientos:
    c. Declaración de la emergencia.
    d. Recuperación de las prestaciones.
    e. Restablecimiento de las condiciones normales.
14. Revisión y simulacro del plan.

En cada punto se deben indicar claramente responsables de cada acción, los que no pueden ser genéricos, es decir “encargado de servidores”, no es útil, se debe indicar nombre, apellido y cargo. En caso de modificación del equipo de trabajo, este documento también debe ser modificado.

Comentarios de la administración

Se realizara la creación de un Plan de Prevención y Recuperación de Desastres, ya que a la fecha el Instructivo de Contingencia que posee el Servicio, es básicamente una acción reactiva ante un incidente y no incluye todo la información desde el punto de vista informático.

III.2. Eliminación, reutilización y devolución de activos de información.

Para todo bien electrónico existe un momento en que su vida útil llega a su fin, sin embargo, este elemento puede contener información sensible que podría poner en dificultades a la institución o al usuario que lo utilizaba, por lo que es importante establecer controles y medidas de seguridad que permitan minimizar la probabilidad de filtración de información. Para esto, el Gore – RM, tiene una norma de eliminación, reutilización y devolución de activos de información.

a.- Observación

Se requiere la implementación de borrados seguros a la información contenida en los equipos. En la actualidad, la normativa establece que una vez que el equipo vaya a ser reutilizado por otro usuario o sea dado de baja, se deben formatear sus medios de almacenamiento, lo cual no es seguro, dado que existen software que permiten la restitución de los datos borrados, incluso cuando el disco duro ha sido formateado en forma normal (no formato rápido).

Riesgos y posibles efectos: Filtración y uso inadecuado de datos confidenciales del Gore – RM.

Nivel de probabilidad de ocurrencia del riesgo: Poco probable.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Moderado.

Recomendación: Se sugiere realizar borrado de archivos seguros utilizando software especializado (los hay de pago como gratuitos para todas las plataformas de sistemas operativos). En casos en la que la información sea en extremo crítica y muy confidencial, utilizar el método gutmann (35 pasadas, el cual es uno de los más seguros, pero también de los más lentos).

Comentarios de la administración

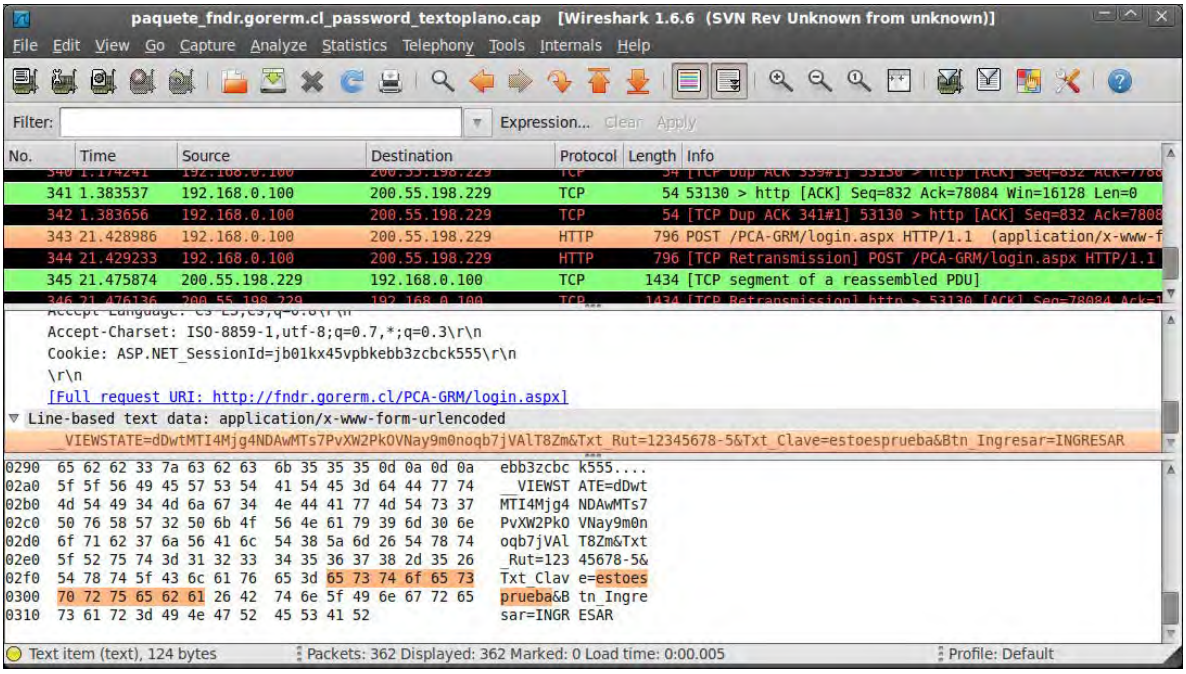
Se realizaran las revisiones de los procedimientos actuales, con el objetivo de realizar las actualizaciones y mejoras necesarias para solucionar estas debilidades, como así mismo se evaluara la adquisición de una herramienta especializada.

III.3. Seguridad de la información "en tránsito".

El "Procedimiento de actualización de seguridad y validación de Data", contiene un punto denominado "controles criptográficos", en su primer punto indica "Todos los sistemas deben tener aplicada criptografía en las passwords".

a.- Observación

Las claves viajan por la red en texto plano, siendo visibles, contrario a lo indicado por el procedimiento. En el Portal de aplicaciones, es posible para un atacante que realice acciones de "hombre en el medio" MITM (técnica que será explicada en el próximo punto), capturar el usuario y contraseña en texto plano y plenamente visible.



Se aprecia en la imagen que el rut de usuario viaja en el campo “Txt_Rut” (rut probado fue 1235678-5) y la clave viaja en texto plano en el campo “Txt_Clave” (clave probada fue estoesprueba, la cual se puede observar claramente).

Esta prueba se llevó a cabo en las dependencias de Baker Tilly Chile, en un ambiente privado y controlado, sin embargo, es repetible en cualquier otra dependencia que no cuente con sistema de detección de intrusos, como por ejemplo en el Gore - RM.

Riesgos y posibles efectos: Acceso desautorizado de la información y pérdida de la integridad de la misma.

Nivel de probabilidad de ocurrencia del riesgo: Probable.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: Para mitigar los riesgos mencionados anteriormente, se sugiere ejectura las siguientes acciones: realizar un hash a la clave del usuario “en el cliente”, por ejemplo utilizando javascript para que la transmisión de la clave no sea en texto plano y posteriormente adaptar los sistemas y servidores a trabajar con HTTPS, es decir web segura, una vez implementado estas mejoras, para un “atacante interno” sería muy difícil conseguir el par “usuario – contraseña” al espiar la red de la institución.

Comentarios de la administración

Se deberá adquirir e implementar un Certificado Digital con el objetivo de minimizar este riesgo y evitar que la información se transfiera como texto plano la red.

III.4. Identificación y autentificación.

Actualmente, en el documento "Norma de uso, identificación y autentificación" se mencionan procedimientos y directrices que son necesarias para la seguridad de la información.

a.- Observación

Durante el proceso de evaluación de la seguridad en la identificación y autenticación, se pudo observar que en los sistemas web no se detecta bloqueo de intentos fallidos de conexión, ya que es posible "probar" contraseñas cuantas veces se desee sin bloqueos.

Riesgos y posibles efectos: Acceso desautorizado de la información y pérdida en la integridad de la misma.

Nivel de probabilidad de ocurrencia del riesgo: Moderado.

Nivel de impacto del riesgo: Menor.

Nivel de severidad del riesgo: Moderado.

Recomendación: Realizar el bloqueo indicado en esta norma, así como modificar la misma e indicar el número exacto de intentos en los que se llevara a cabo el bloqueo (lo aconsejable son 3 intentos).

Comentarios de la administración

En el desarrollo del nuevo Portal de Aplicaciones, se encuentra considerada la implementación del bloqueo cuenta a los 3 intentos, debiendo posterior a esto solicitar al Depto. de Informática el desbloqueo de la dirección IP.

b.- Observación

En la normativa vigente se indica que las contraseñas deben contar con una longitud mínima de 8 caracteres, incluidas letras mayúsculas, minúsculas, dígitos, símbolos y "no deben ser fáciles de adivinar". Sin embargo, al utilizar la información que se obtuvo al acceder en la red interna, ítem que se explicará en detalle en el punto III.6., se puede observar que esto no se cumple (repitiendo la información del punto indicado y enfocado en las cuentas de correo):

USER: ccampero PASS: 123gob
USER: mbarraza PASS: 123gob
USER: cphs PASS: 123gob
USER: melgueta PASS: 123gob
USER: ccartes@gobiernosantiago.cl PASS: 123gob
USER: amunoz@gobiernosantiago.cl PASS: 123gob
USER: scorrea@gobiernosantiago.cl PASS: 123gob
USER: ptorrealba@gobiernosantiago.cl PASS: ptorrealba2k11
USER: amunozz@interior.gov.cl PASS: amunozz2k12
USER: jmoraga@gobiernosantiago.cl PASS: pukona27
USER: rcathalifaud PASS: rc78lk
USER: pmendoza PASS: Vi7ruvi0

Como se puede observar, la contraseña 123gob es común para múltiples usuarios y no cumple con la norma, las contraseñas de ptorrealba y amunozz son en gran parte el mismo nombre de usuario, la única contraseña que se acerca a la norma es la del usuario pmendoza, pero le falta algún símbolo.

Riesgos y posibles efectos: Acceso desautorizado de la información y pérdida de la integridad en la misma.

Nivel de probabilidad de ocurrencia del riesgo: Probable.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: Se sugiere realizar un cambio total de todas las cuentas de usuarios, tanto en el correo institucional como en los sistemas que velar por el cumplimiento de la norma indicada.

Comentarios de la administración

En el desarrollo del nuevo Portal de Aplicaciones, se encuentra considerada la implementación de contraseña de un largo de 8 caracteres , que deberá contener Letras, Números y Símbolos, que expirara en forma automática en 90 días y que no se podrá repetir la contraseña anterior al ser modificada.

Este mismo modelo es el que se implementará para las cuentas de correo electrónico.

c.- Observación

No se realizan cambios de las contraseñas de acceso. Además, la norma no especifica que todos los usuarios deberían cambiar obligatoriamente su contraseña cada cierta cantidad de meses (3 se ajusta al estándar empresarial).

Riesgos y posibles efectos: El principal problema de esta situación consiste en que el usuario no es obligado, en ningún momento, a modificar su clave de acceso, de manera que se facilita la revelación o filtración de las password, arriesgando con ello acceso a información confidencial de la empresa y pérdida en la integridad de los datos.

Nivel de probabilidad de ocurrencia del riesgo: Moderado.

Nivel de impacto del riesgo: Menor.

Nivel de severidad del riesgo: Moderado.

Recomendación: Se propone modificar la normativa y realizar estos cambios a la brevedad, esto aplica en todos los sistemas y servicios incluidos sistemas web, cuentas de correo, etc.

Comentarios de la administración

En el desarrollo del nuevo Portal de Aplicaciones, se encuentra considerada la implementación de contraseña de un largo de 8 caracteres , que deberá contener Letras, Números y Símbolos, que expirara en forma automática en 90 días y que no se podrá repetir la contraseña anterior al ser modificada.

Por lo que al primer ingreso una vez puesto en marcha este nuevo Portal de aplicaciones, se les obligara a realizar el cambio de su contraseña actual, bajo los parámetros antes mencionados.

d.- Observación

Se utilizan cuentas genéricas. La norma indica que no se deben usar cuentas fáciles de predecir, con nombres de usuarios predeterminados como anónimo, invitado, etc., a pesar de ello, es posible acceder al servicio ftp del servidor 200.75.2.62 (Firewall 2da capa GORE) usando la cuenta anónima (anonymous). Aunque la información contenida no es crítica, siempre es un factor de riesgo tener estas cuentas abiertas.

Riesgos y posibles efectos: Filtración de información confidencial.

Nivel de probabilidad de ocurrencia del riesgo: Poco probable.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Moderado.

Recomendación: Se sugiere el cierre del servicio ftp de este servidor si es que no es necesario, en caso contrario, deshabilitar el ingreso anónimo.

Comentarios de la administración

Se bloqueara en forma inmediata el acceso de la cuenta anónima (anonymous), en el servidor ftp analizado y se realizaran las revisiones correspondientes en todos los servidores y servicios para el bloqueo de este tipo de cuentas.

III.5. Encargado de Seguridad (oficial de seguridad).

En distintos documentos se hace mención del "encargado de seguridad", cargo que actualmente recae sobre el Señor Patrick Stockins, quien a su vez es el Jefe División de Administración y Finanzas.

a.- Observación

Durante el proceso de evaluación de la seguridad en la identificación y autenticación, se pudo observar que la división que el Señor Stockins lidera actualmente, es la misma que controla al Área de Informática. Normalmente, el cargo de "encargado de seguridad" recae sobre una o más personas cuya única labor es la de ejercer este cargo, según las buenas practicas, esta persona debe depender directamente del Área de Auditoria Interna, no poseer posibles conflictos de intereses y tener los conocimientos informáticos suficientes para realizar test de penetración, de stress, etc., así como también tener conocimientos en la gestión de proyectos, ya que trabajaría a la par con el Área de informática, en el control y avance de las mejoras propuestas.

Riesgos y posibles efectos: Se pueden generar conflictos de intereses, debido a que la persona encargada de evaluar la seguridad es la misma que está a cargo de la jefatura del área evaluada.

Nivel de probabilidad de ocurrencia del riesgo: Probable.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: Con el fin de minimizar los riesgos mencionados, se recomienda realizar las gestiones necesarias para crear este cargo a la brevedad, este candidato puede ser una persona natural, así como también una empresa externa experta en el tema, que brinde dicho servicio.

Comentarios de la administración

Se hará presente esta observación a la plana directiva del servicio para su consideración y decisión.

III.6. Evaluación de la red institucional.

Objetivo de auditoría: El equipo auditor evalúa la seguridad de las comunicaciones, los datos transmitidos, los dispositivos usados durante la transmisión, la documentación necesaria para la realización eficiente e ininterrumpida de esta transmisión, y los sistemas utilizados para la transmisión de datos de un entorno a otro, comprobando el cumplimiento de las normativas de seguridad de la información.

En esta actividad, equipo auditor solicitó conexión a la red institucional, sin tener privilegios especiales, tal y como si fuera un usuario más, con el fin de revisar las acciones que un mal intencionado interno pudiera realizar. Cabe destacar que según distintos estudios se asegura que alrededor del 70% de los ataques son realizados por personal interno de las instituciones.

a.- Observación

Falta un sistema de detección de "intrusos" en la red interna de Gore – RM. Tras una revisión al interior de la red de la institución, fue posible realizar un ataque de hombre en el medio (MITM, intervenir las conexiones de todos los equipos conectados a la red para averiguar información sensible, como contraseñas de todos los equipos conectados, esta acción se llevó a cabo teniendo los mismos privilegios que cualquier usuario promedio conectado a la red interna del Gore - RM).

Dado que ataques de este tipo en redes medianas a grandes puede generar pérdida de paquetes o lentitud en la actividad normal de la red, esta acción se realizó sólo por 10 minutos, durante los cuales fue posible obtener las siguientes claves:

POP : 10.13.10.9:110 -> USER: rcathalifaud PASS: rc78lk
POP : 10.13.10.9:110 -> USER: ccampero PASS: 123gob
POP : 10.13.10.9:110 -> USER: mbarraza PASS: 123gob
POP : 10.13.10.9:110 -> USER: scorrea@gobiernosantiago.cl PASS: 123gob
POP : 10.13.10.9:110 -> USER: pmendoza PASS: Vi7ruvi0
POP : 10.13.10.9:110 -> USER: ptorrealba@gobiernosantiago.cl PASS: ptorrealba2k11
POP : 190.160.0.137:110 -> USER: pablotorrealba@vtr.net PASS: pasena.oxcomj.1084
POP : 10.13.10.9:110 -> USER: ccartes@gobiernosantiago.cl PASS: 123gob
POP : 10.13.10.9:110 -> USER: cphs PASS: 123gob
POP : 10.13.10.9:110 -> USER: melgueta PASS: 123gob
POP : 10.13.10.9:110 -> USER: jmoraga@gobiernosantiago.cl PASS: pukona27
POP : 10.13.210.43:110 -> USER: amunozz@interior.gov.cl PASS: amunozz2k12
POP : 10.13.10.9:110 -> USER: amunoz@gobiernosantiago.cl PASS: 123gob

Así mismo, fue posible obtener otro tipo de información, como por ejemplo, que páginas web se estaban visitando algunos de los usuarios, tal como se detalla a continuación:

- pmendoza1.stgo.rm - - [19/Jul/2012:14:25:59 -0400] "GET http://images.lun.com/lunservercontents/FlashObjectProduction/FlippingHomePage/XML/2012/jul/19/hojear_1024_0_0.xml HTTP/1.1" - - "http://www.lun.com/FlashObject/hojearPortada.swf" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)".
- ptorrealba.stgo.rm - - [19/Jul/2012:14:26:11 -0400] "GET http://notify11.dropbox.com/subscribe?host_int=208685274&ns_map=119709216_1241365257760&ts=1342722213 HTTP/1.1" - - "-" "-"
- bmedina1.stgo.rm - - [19/Jul/2012:14:30:43 -0400] "GET http://ads.mapcity.com/www/delivery/afr.php?refresh=30&zoneid=3&cb=INSERT_RANDOM_NUMBER_HERE&loc=http%3A%2F%2Fwww.mapcity.cl%2F HTTP/1.1" - - "http://ads.mapcity.com/www/delivery/afr.php?refresh=30&zoneid=3&cb=INSERT_RANDOM_NUMBER_HERE&loc=http%3A%2F%2Fwww.mapcity.cl%2F" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB7.3; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.1; .NET4.0C; .NET4.0E)"

Riesgos y posibles efectos: Acceso desautorizado a la información y filtración de datos, así como la probabilidad de pérdida de la integridad de los datos.

Nivel de probabilidad de ocurrencia del riesgo: Probable.

Nivel de impacto del riesgo: Moderado.

Nivel de severidad del riesgo: Alto.

Recomendación: Con el fin de minimizar los riesgos mencionados anteriormente, se sugiere implementar un sistema de detección y prevención de intrusos para la red interna, además, proceder a modificar las claves de los usuarios indicados en este punto.

Comentarios de la administración

Se realizara las revisiones y análisis correspondientes, para posteriormente evaluar la adquisición e implementación de solución de detección de intrusos para la red interna del Servicio.

Confianza, Visión y Resultados

BAKER TILLY CHILE

AUDIT, TAX & CONSULTING

Plan de Mejoras

Gobierno Regional Metropolitano de Santiago

GUERRA & RABY

an independent member of BAKER TILLY INTERNATIONAL

Santiago, 13 de julio del 2012

Señores
Gobierno Regional Metropolitano de Santiago.
Presente

Estimados Señores:

Tenemos el agrado de presentar a vuestra consideración el plan de mejoras desarrollado para el Gobierno Regional Metropolitano de Santiago, en adelante, Gore - RM.

El presente plan fue desarrollado en base a las vulnerabilidades detectadas durante el Proceso de Auditoría de Procesos TI y Plan de Mejoras de Sistemas Informáticos, considerando una selección de puntos de la Norma Chilena – ISO 27001 (que a la vez son puntos considerados claves en la Norma ISO 27002), los que estimamos necesarios para una primera iteración de la misma y considerando plazos razonables para la envergadura de la institución.

Quedamos a su disposición para ampliar y/o aclarar el contenido del plan.
Saludamos muy atentamente a ustedes,

Marco Antonio Halal Manzano

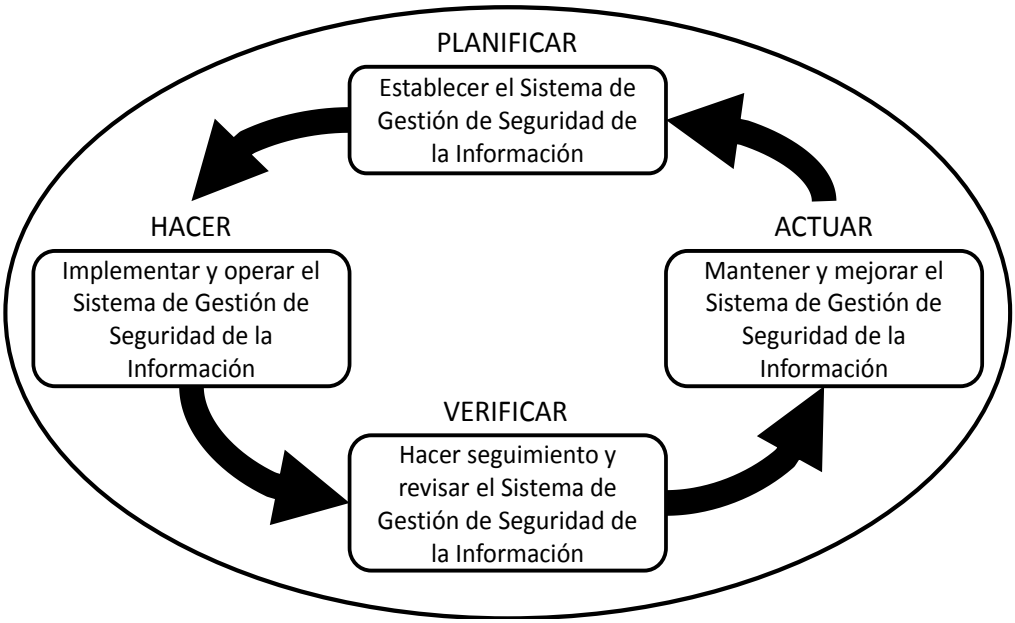
Baker Tilly Chile

Contenido

PLAN DE MEJORAS

Capítulo I. Introducción

En la Norma Chilena – ISO 27001 propone adoptar un modelo de proceso iterativo consistente en Planificar – Hacer – Verificar – Actuar (PHVA):



Dado que en la actualidad ya existen políticas y normas tendientes a implementar "Seguridad de la Información", no se comenzará desde cero, efectivamente hay mejoras por realizar, pero la existencia de estos documentos indica que en la institución ya hay conciencia de la importancia de este punto.

Para ayudar al Gore - RM en esta tarea proponemos el siguiente plan de mejoras que establece las prioridades de las acciones que se deben llevar a cabo por parte de la institución, acorde a la experiencia del equipo auditor, debilidades detectadas y una selección de puntos de la Norma NCH ISO 27001 (que a la vez son puntos considerados claves en la Norma ISO 27002) considerados necesarios de abordar para una primera iteración.

Capítulo II. Acciones a realizar

Las siguientes actividades a mejorar están ordenadas de acuerdo a la criticidad que el equipo auditor considera necesario para mejorar la seguridad informática en el Gore – RM.

II.1. Autentificación de usuarios

Punto A.11.4.2 nch27001:

"Se deben usar métodos de autentificación apropiados para controlar el acceso de usuarios remotos".

Dada la falencia de seguridad en el Portal de Aplicaciones, la cual permite a un usuario no autorizado ingresar sin saber la clave del usuario suplantar.

Plazo máximo sugerido para solucionar: 4 semanas.

II.2. Validación de los datos de entrada

Punto A.12.2.1 nch 27001:

"Validación de los datos de entrada".

En concordancia con el punto anterior, y viendo que es posible realizar inyecciones SQL en el Portal de Aplicaciones y en algunos de los sistemas contemplados en el mismo, es necesario que el área de desarrollo realice modificaciones en las funciones que realizan consultas a las bases de datos para asegurar que no es posible realizar acciones indebidas, en casi todos los lenguajes de programación existen funciones predeterminadas que permiten disminuir la probabilidad de que un atacante realice inyecciones de SQL, por ejemplo, en java "PreparedStatement", en C# "PreparedStatement", etc.

Plazo máximo sugerido para solucionar: 8 semanas.

Observación: En este punto también aplica el ítem A.10.4.1. "Controles contra el código malicioso".

II.3. Trabajo remoto

Punto A.11.7.2 nch 27001:

"Se debe desarrollar e implementar una política, y procedimientos y planes de operaciones de actividades de trabajo remoto".

En este punto, consideramos necesario que se estudie en forma interna y luego se documente, la necesidad de que los sistemas de "Back office" del GoreRM estén disponibles en internet, en recomendación del equipo auditor, estos servicios deberían de ser accesibles sólo en las dependencias del Gore - RM y en el caso particular de que algún usuario necesite realizar tareas en forma remota, acceder primero a una red privada virtual segura (VPN) para luego poder ingresar a los sistemas.

Plazo máximo sugerido para solucionar: 12 semanas.

Observación: En este punto también aplica el ítem A.11.6.2 "Aislamiento de sistemas sensibles".

II.4. Controles de red

Punto A.10.6.1 nch 27001:

"Las redes se deben gestionar y controlar adecuadamente, para protegerlas contra amenazas, y mantener la seguridad de los sistemas, incluyendo la información en tránsito".

Dado que los sistemas web del Gore - RM viajan en forma plana por el puerto 80 (http), y que es posible realizar ataques de "Hombre en el medio" al interior de las dependencias (escuchar la comunicación), una persona maliciosa podría obtener información sensible, desde contraseñas hasta datos propios de los sistemas, por lo que creemos necesario que se habilite http seguro (https) con los certificados (ssl) digitales pertinentes para asegurar razonablemente que aunque alguien capture la "conversación" no pueda interpretarla correctamente. Estos certificados se pueden autogenerar o bien, ser obtenidos mediante una "autoridad certificadora" reconocida (los costos asociados dependen entre las distintas entidades).

Plazo máximo sugerido para solucionar: 20 semanas.

II.5. Seguridad de los servicios de red

Punto A.10.6.2 nch 27001:
"Las características de la seguridad, los niveles del servicio, y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en cualquier acuerdo de servicios de red".

El equipo auditor considera necesario que se replanteen los controles que se deben llevar a cabo en el control y gestión de la red, así mismo, cree necesaria la implementación de un sistema de detección de intrusos (IDS/IPS) que permita controlar acciones que no deberían ocurrir al interior de la red como intervenciones en las transacciones, etc.

Plazo máximo sugerido para solucionar: 24 semanas.

Observación: En este punto también aplica el ítem A.10.8.4. "Mensajería electrónica".

II.6. Sistema de gestión de contraseñas

Punto A.11.5.3 nch 27001:
"Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad"

Según normativa interna, la contraseña puede ser cambiada mediante solicitud al área de informática, a pesar de que hay una normativa que indica la "fortaleza mínima" de seguridad en la contraseña se verificó que no siempre se respeta, así como tampoco el cambio periódico de las mismas, por lo que es necesario que se cambien todas las contraseñas, de todos los sistemas y cuentas de correo electrónico de los usuarios.

Plazo máximo sugerido para solucionar: 24 semanas.

Observación: En este punto también aplica el ítems A.11.3.1 "Uso de contraseñas".

II.7. Segregación de funciones

Punto A.10.1.3 nch 27001:
"Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización".

En referencia con la doble labor del Jefe de la División de Administración y Finanzas, quien a la vez desempeña labores de Oficial de Seguridad de la información, recomendamos realizar la búsqueda del candidato ideal para el cargo de "Oficial de seguridad", ya sea una persona natural o una empresa experta en seguridad informática que brinde este servicio. A su vez, este candidato debe ser depend6iente del Área de Auditoria Interna. Por otra parte, aunque se cuenta con servidores de desarrollo, el equipo a cargo de esto no debería de tener ningún acceso a los servidores de producción, por lo que es necesario segregar esta función.

Plazo máximo sugerido para solucionar: 32 semanas.

Observación: Este punto también aplica en el ítem A.6.1.3. "Asignación de responsabilidades sobre la seguridad de la información".

II.8. Respaldos de la información

Punto A.10.5.1 nch 27001:
"Se deben hacer regularmente copias de seguridad de la información y del software y probarse regularmente acorde con la política de respaldo".

Existe una política de respaldos, pero no hay gestión sobre ella, no se respeta la periodicidad de los respaldos externos, es necesario que se verifique el cumplimiento de la periodicidad y las pruebas que se deben realizar sobre los respaldos.

Plazo máximo sugerido para solucionar: 8 semanas.

II.9. Seguridad en la reutilización o descarte de equipos

Punto A.9.2.6 nch 27001:
"Todo aquel equipamiento que contenga medios de almacenamiento se debe revisar para asegurar que todos los datos sensibles y software licenciado se hayan removido o se haya sobrescrito con seguridad antes de si descarte o baja".

Dentro de las normas actuales del Área Informática se indica que en estos casos el equipo debe ser "formateado", sin embargo esto no es un método seguro de eliminación de información, por lo que se recomienda que frente a todos los medios de almacenamiento, discos duros internos, discos duros removibles, pendrives, cintas magnéticas, etc. La información sea borrada en forma segura utilizando los métodos indicados en el informe de Auditoría de Procesos TI y Plan de Mejoras de Sistemas Informáticos. En caso de discos ópticos como CD o DVD se recomienda eliminación por fuego.

Plazo máximo sugerido para solucionar: 4 semanas.

Observación: Este punto también aplica al ítem A.10.7.2. "Eliminación de los medios".

II.10. Desarrollo e implementación de planes de continuidad que incluyen seguridad de la información

Punto A.14.1.3 nch 27001:
"Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información al nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla de los procesos críticos del negocio".

Se recomienda implementar un Plan de Prevención y Recuperación ante Desastres, tal y como se indica en el informe de Auditoría de Procesos TI y Plan de Mejoras de Sistemas Informáticos.

Plazo máximo sugerido para solucionar: 24 semanas.

Observación: Este punto también aplica al ítem A.13.2.1. "Responsabilidades y procedimientos", así como también al ítem A.13.2.2. "Aprendiendo de los incidentes de seguridad de la información" y al ítem A.13.2.3. "Recolección de evidencia".

II.11. Verificación del cumplimiento técnico

Punto A.15.2.2 nch 27001:
"Se deben verificar regularmente los sistemas de seguridad en cuanto a su conformidad con las normas de seguridad de la información implementadas".

Todas las normas existentes, más las modificaciones recomendadas, se deben verificar en forma técnica en un plazo máximo de 1 vez por año.

Plazo máximo sugerido para solucionar: 48 semanas.

II.12. Revisión independiente de la seguridad de la información

Punto A.6.1.8 nch 27001:
"El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se debe revisar en forma independiente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad".

Recomendamos en un plazo de un año, realizar una Auditoría de Seguridad Informática externa para hacer un seguimiento a las falencias detectadas en el informe de auditoría actual, más las mejoras propuestas por este documento para así concluir la primera iteración en el modelo propuesto por la Norma NCH ISO 27001, además adicionar nuevos objetivos de control y controles para cumplir con el proceso iterativo-incremental.

Plazo máximo sugerido para solucionar: 52 semanas.

II.13. Registros de Auditoria

Punto A.10.10.1 nch 27001:
"Se deben elaborar registros de auditoría de las actividades de usuarios, excepcionales y eventos de seguridad de la información, y se deben mantener durante un periodo acordado para ayudar a futuras investigaciones y en la supervisión del control de acceso".

Aproximadamente el 95% de los escaneos e intentos de acceso que el equipo auditor realizó fueron desde las dependencias de Baker Tilly Chile, donde contamos con ip fija, por lo que si se controlaran los logs de los servidores podrían haber bloqueado esta dirección, sin embargo, esto no ocurrió, por lo que recomendamos crear un procedimiento que indique quien es el responsable

de realizar estas labores (revisión de logs de los servidores y eventos importantes), así como la periodicidad que debe realizar esta actividad.

Plazo máximo sugerido para solucionar: 40 semanas.

III. Plazos estimados

La siguiente Carta Gantt, especifica un estimado de los plazos en los cuales los puntos (ordenados por prioridad) deberían de estar solucionados y no en base a cuánto podría demorar cada actividad, ya que esto sólo lo podrían saber en el área de informática del Gore - RM.

Id.	Nombre de tarea	Comienzo	Fin	Duración
1	Autentificación de usuarios	13-07-2012	09-08-2012	4s
2	Validación de los datos de entrada	13-07-2012	06-09-2012	8s
3	Trabajo remoto	13-07-2012	04-10-2012	12s
4	Controles de red	13-07-2012	29-11-2012	20s
5	Seguridad de los servicios de red	13-07-2012	27-12-2012	24s
6	Sistema de gestión de contraseñas	13-07-2012	27-12-2012	24s
7	Segregación de funciones	13-07-2012	21-02-2013	32s
8	Respaldos de la información	13-07-2012	06-09-2012	8s
9	Seguridad en la reutilización o descarte de equipos	13-07-2012	09-08-2012	4s
10	Desarrollo e implementacion de planes de continuidad que incluyen seguridad de la información	13-07-2012	27-12-2012	24s
11	Verificación del cumplimiento técnico	13-07-2012	13-06-2013	48s
12	Revisión independiente de la seguridad de la información	13-07-2012	11-07-2013	52s
13	Registros de auditoría	13-07-2012	18-04-2013	40s