**SECURESOFT CORPORATION**

**e-Secure Consulting Group**

**REPORTE SEMANAL**

**PLATAFORMA PATCH MANAGEMENT GFI LANGUARD**

**Preparado para:**



**Fecha:**

**${fecha\_actual}**

****

**El presente documento contiene información estrictamente privada y confidencial para Securesoft Corporation S. A. C. y Banco Ripley.**

1. **OBJETIVO**

Este documento servirá como herramienta para verificar el estado de la plataforma de seguridad y su correcto funcionamiento.

1. **ALCANCE**

Este documento dará a conocer el estado de la plataforma GFI Languard.

1. **ESTADO DE LA PLATAFORMA**

**SISTEMA OPERATIVO**

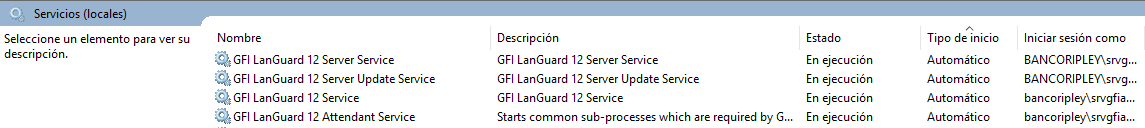
* **Recursos**

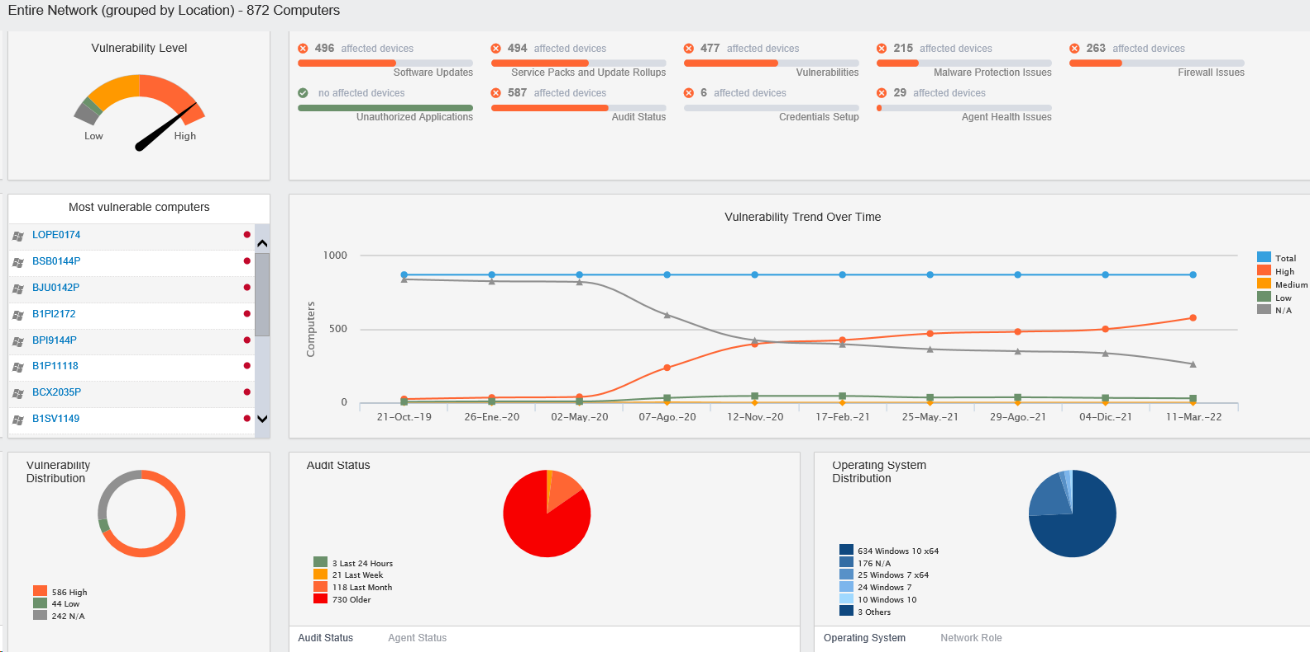
${graph2308}

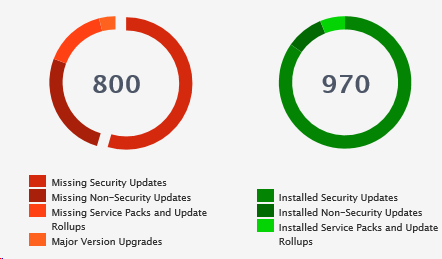
* El uso promedio de CPU, durante la semana fue 4.36%.
* El uso promedio de Memoria, durante la semana fue 69.18%.
* El uso promedio de Disco C: durante la semana fue 70.88%.
* El uso promedio de Disco D: durante la semana fue 6.44%.

**GFI Languard y Central Management Server**

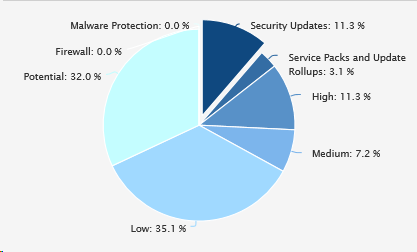
* Se muestra que los servicios asociados a los componentes GFI Languard y Central Management Server se encuentran en ejecución:



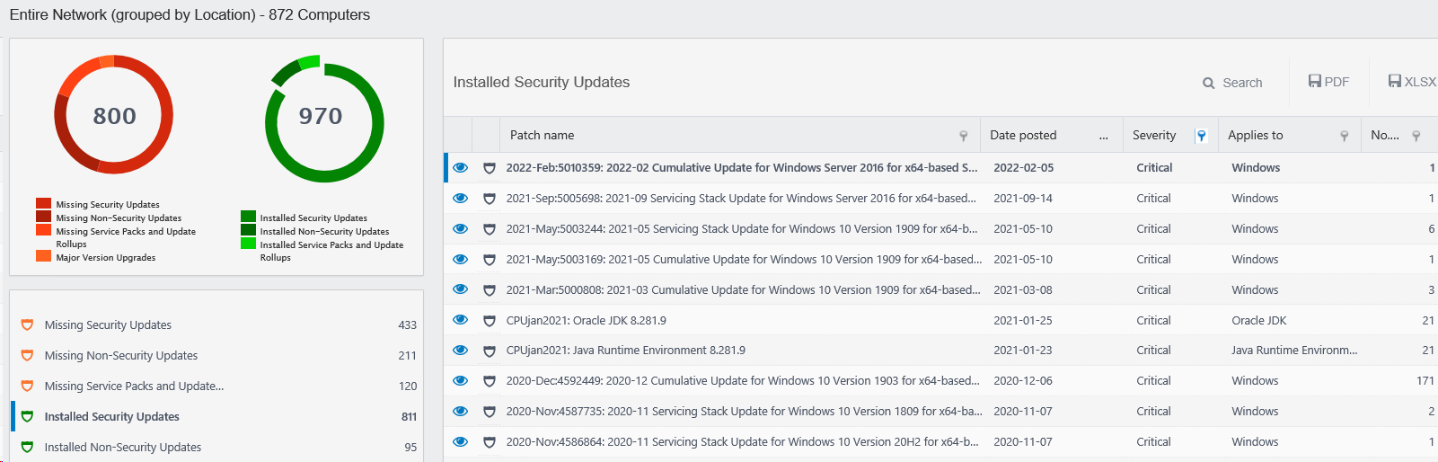
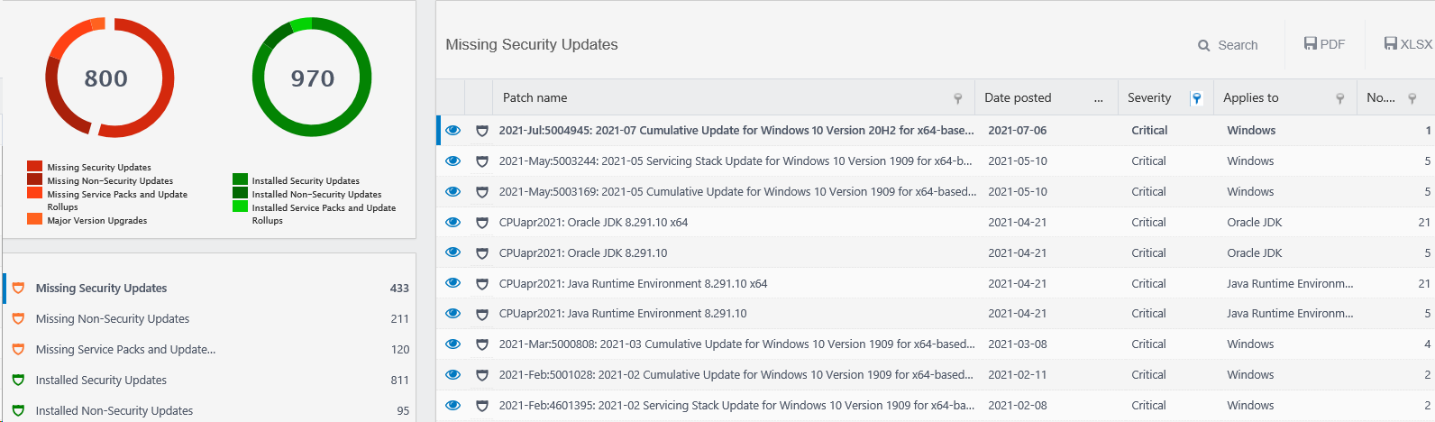
* Se muestra que la consola de GFI Languard tiene administrando 872 equipos del dominio Banco Ripley, las cuales fueron sincronizadas del directorio activo el mismo día de elaboración del informe. De las cuales 118 computadoras fueron auditadas en el último mes.
* Se muestra que tiene instalados 800 parches de seguridad y falta desplegar 970 parches de seguridad en la red.
* Observación: Actualmente no se están distribuyendo parches de ningún tipo, por lo que esta cifra solo variaría dependiendo de los parches instalados a través de Windows update o el Wsus. Además, esta cifra solo abarca los equipos que fueron auditados. Por lo que esta cifra aumentara cuando se reanude los escaneos.



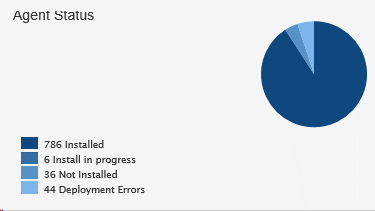
* Se muestra que el 35.1% de parches de Microsoft pendientes son de categoría baja.   
  Nota: Según Microsoft los parches Críticos e Importantes corresponden a parches de seguridad ([Fuente](https://www.microsoft.com/en-us/msrc/security-update-severity-rating-system))



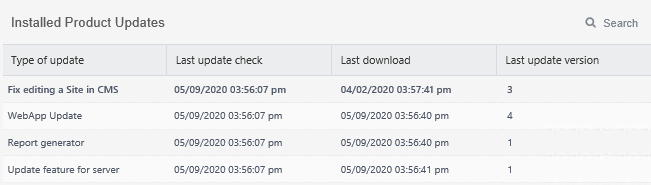
* Se muestra un Top 10 de las actualizaciones de seguridad para Windows pendientes e instaladas, con mayor alcance de equipos.



* La cantidad de agentes instalados es 786.
* La cantidad de agentes con instalación en curso es 6.
* La cantidad de agentes en desinstalación en curso es 0.
* Hay 36 equipos con instalación pendiente y 44 que corresponde a errores en la instalación.

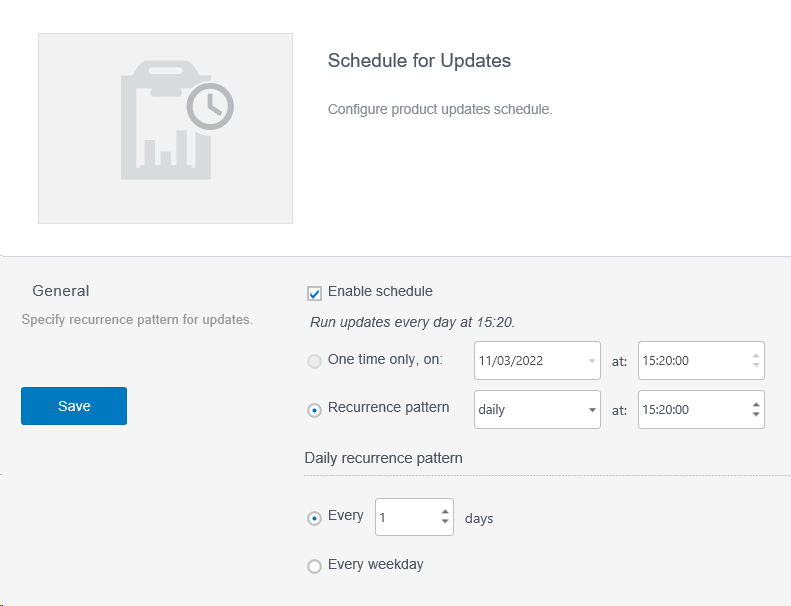


* Se evidencia que el sistema GFI Languard se encuentra actualizado al 09/05/2020.  
  Nota: Debido a que las definiciones de parches disponibles se sincronizan automáticamente con los relay agents ni bien se realizaban esta actualización al medio día. Se cambió la configuración de actualizaciones de diaria a las 11am a semanal siendo el domingo a la 1am cuando inicie esta actualización. Esto para evitar que ocurra tráfico por la WAN debido a las actualizaciones que antes eran diarias.



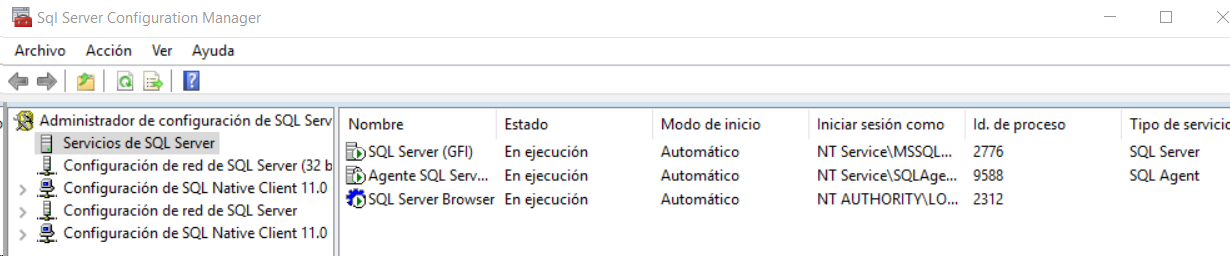
**Horario de actualización de agentes:**

* Se mantiene fijo como configuración para los agentes que el horario que tienen permitido recibir actualizaciones del servidor principal es a las 15:20:00 diario.



**Base de Datos**

* Se evidencia que los servicios de base de datos SQL Server se encuentran en ejecución.



**CONCLUSIONES**

* Se observó que los servicios internos de la plataforma GFI Languard se encuentra funcionando de forma correcta.
* El consumo de Memoria del Servidor GFI, durante la semana fue de 69.18%.
* El consumo de la partición “Disco local (C:)” del Servidor GFI, durante la semana fue de 70.88%.
* El consumo de la partición “Nuevo vol (D:)” del Servidor GFI, fue 6.44%.

1. **RECOMENDACIONES**

* Se recomienda aplicar límites de ancho de banda, del lado de los equipos de comunicaciones del cliente, para conexiones desde las sedes del banco con el servidor de GFI Languard (172.17.6.141). Según lo conversado con personal de comunicaciones el consumo permitido debería de ser menor o igual al 75% del ancho de banda disponible para la sede.
* Debido a que la sede central cuenta con una conexión simétrica de 50Mbps, se recomienda aplicar un límite igual o menor a 37.5Mbps (75% del total) para las conexiones WAN salientes y entrantes que apunten al servidor de GFI Languard (172.17.6.141).

**NOTA: Es importante aplicar estas recomendaciones debido a que la solución no cuenta con límites de consumo de ancho de banda, solo de horarios.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTROL DE CAMBIOS** | | | | |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| 00 | ${autor} | Supervisor CyberSOC | 18/03/2022 | Actualización de estado de la herramienta |