



Auditoría al Sistema de Información “Starship”

ETAPA 6 - Obtención de los resultados
Conformado por: Grupo 1 y Grupo 17



Vimos en la etapa anterior...

- Pruebas de verificación de cumplimiento de los objetivos de control de acuerdo al ámbito a evaluar.
- Controles diseñados para el cumplimiento de sus fines y para probar su adecuado funcionamiento.



Obtención de resultados

¿Cuál es el propósito de esta etapa ?

Esta etapa tiene como propósito obtener los resultados de las aplicaciones de los :

- Procedimientos de control
- Pruebas realizadas



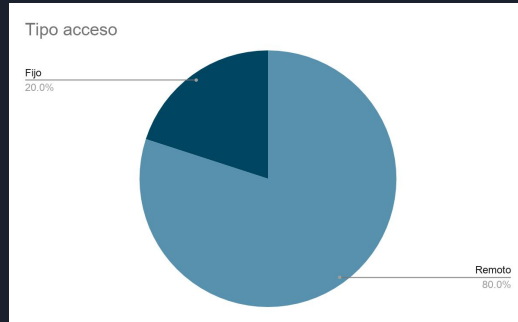
Control Acceso Virtual

Para el control de acceso virtual empresa dispone :

- Aplicación acceso remoto :
 - cada dispositivo personal o corporativo cuenta con un cliente instalado de la aplicación Cisco AnyConnect Secure Mobility
- Credenciales :
 - los empleados deben ingresar sus credenciales (username y password), las username es el mail corporativo
- Registro :
 - la aplicación persiste en los logs de la aplicación datos de usuario, ip , hora de conexión , hora de desconexión .

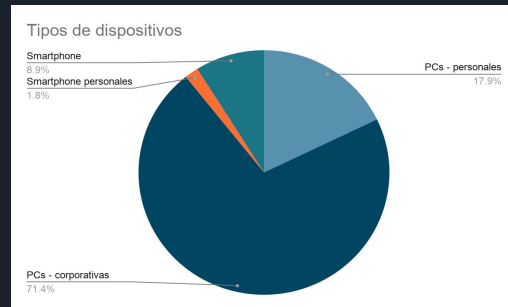
Resultados - Control Acceso Virtual (*)

- Se confía en los controles asumiendo un riesgo bajo



Resultados acceso:

- Acceso Remoto : 80 % (280 empleados)
- Acceso Fijo : 20 % (70 empleados)



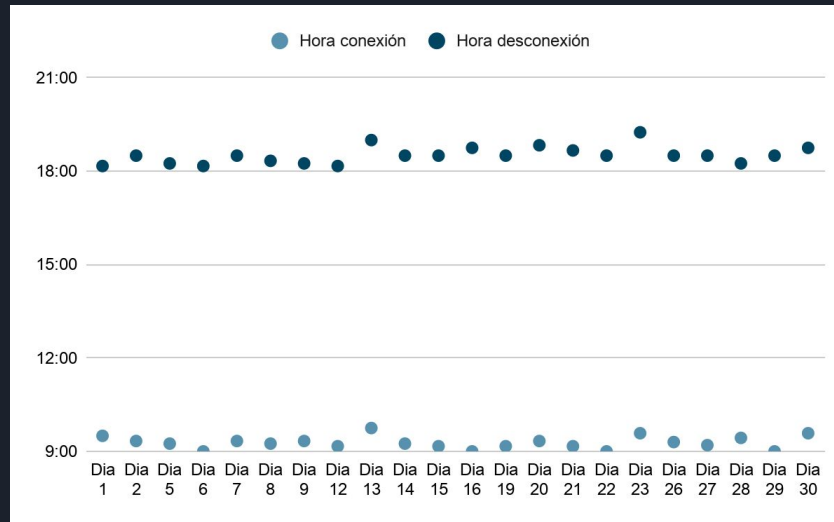
Resultados por tipos dispositivos:

- PCs : 89,30 % (280 disp)
 - Corporativas 71,4 % (200)
 - Personales : 17,9 % (50)
- Smartphones : 10,70 % (30)
 - Corporativas 8,9 % (25)
 - Personales : 1,8 % (5)

(*) valores medio - Abril 2021

Resultados - Control Acceso Virtual (*)

- Se reevalúa los riesgos en los controles y se establece aumentar la confianza de los mismos.
- Testeo sustantivo limitado :
 - Testeo control de hs conexión / desconexión



(*) valores medio - Abril 2021



Resultados - Control Acceso físico

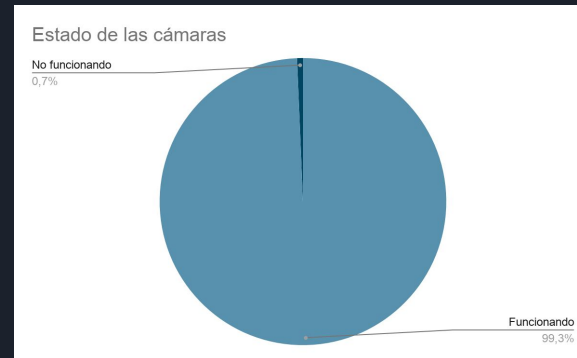
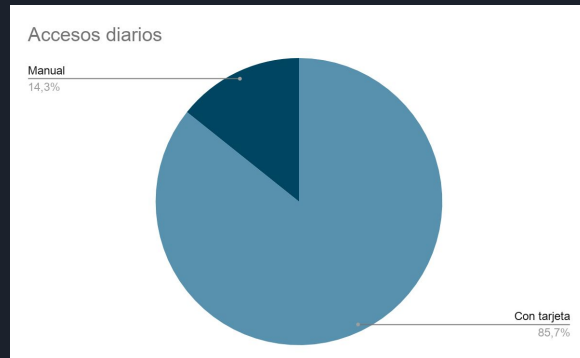
Para el control de acceso físico la empresa aplica

- **Tarjeta RFID:** Cada empleado cuenta con una tarjeta RFID, en caso de extravío u olvido de la tarjeta se hace una carga manual de la entrada y salida del empleado por el personal de seguridad.
- **Personal de seguridad:** Para acceder a las instalaciones existen dos guardias que se encargan de constatar que la persona que está ingresando coincide con la tarjeta, para ello cuentan con un monitor donde se visualizan los datos del individuo al momento de pasar la tarjeta por el lector.
- **Fecha y hora de entrada:** Se registra la fecha y hora de ingreso, también al dejar el edificio.
- **Niveles de seguridad:** Cada tarjeta adjudica permisos los cuales permiten ingresar a distintas áreas.
- **Cámaras de seguridad:** En las entradas y dentro del edificio existen cámaras de seguridad que graban la actividad.

Resultados - Control Acceso físico (*)

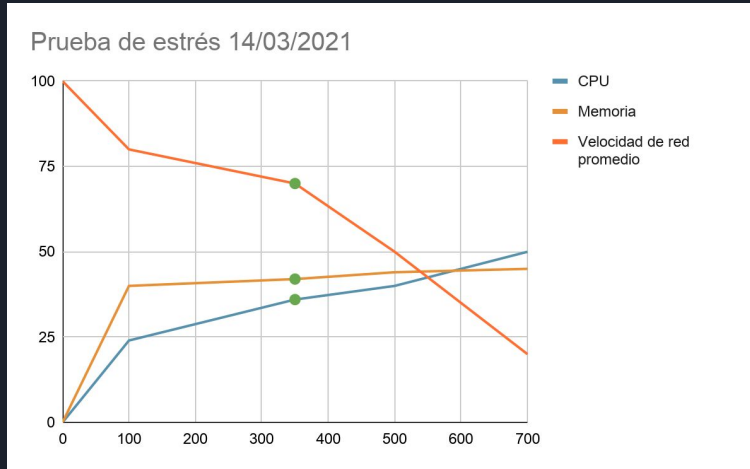
- Se audita el sistema que registra la entrada. No se encontraron irregularidades
- Se verificó el funcionamiento de las cámaras. Solo una de ellas no funcionaba correctamente, igualmente la cámara defectuosa no registraba un riesgo.
- Se intentó ingresar a una sala sin los permisos requeridos. No fue posible
- Se entrevistó al personal de seguridad sobre el protocolo. fueron solventes.
- Se entrevistaron a distintos empleados sobre qué ocurría si olvidaban su tarjetas. Todos respondieron correctamente.

En base a los datos y las entrevistas realizadas se decidió **confiar** en este control.



Resultados - Control de la red

La empresa realiza periódicamente pruebas de estrés sobre la red con el objetivo de analizar cuántos empleados pueden acceder concurrentemente y mantener la operatividad sin fallas.



Resultados para 350 empleados:

- CPU: 36 %
- Memoria: 42 %
- Velocidad de red promedio: 70 % de su capacidad



Resultados - Control de la red

Para complementar los resultados se decidió analizar registros de reclamos de los empleados relacionados a problemas por conexión de red y/o lentitud en el sistema.

El análisis determinó que durante los últimos 6 meses se reportaron 10 problemas de conexión de red los cuales fueron resueltos marcados como: “falla de conexión externa por problemas de internet con la red hogareña del empleado”

Los resultados validan las pruebas de estrés previas y podemos concluir en que la red trabajaría en **valores inferiores al 50 % de su capacidad máxima** para 350 empleados conectados.

Los resultados del test de control de la red validaron la confianza que se definió previamente y su **alta** efectividad como control preventivo.



Controles de Recursos - a la Gerencia

Control de criterios de asignación de recursos

Se cumplieron con todos los criterios preestablecidos para la asignación de los recursos destinados a la gerencia.

Control de características de los recursos

Se cumplieron correctamente con las características de Hardware y Software preestablecidas para los recursos destinados a la gerencia.

Control de tiempos para la entrega

Se cumplieron correctamente con los tiempos preestablecidos para la entrega de los recursos destinados a la gerencia.



Controles de utilización de recursos - a la Gerencia

Control de tareas realizadas

Los empleados gerenciales pueden realizar correctamente todas las tareas correspondientes con el recurso otorgado por la empresa.

Control de aplicaciones instaladas

Los controles se realizan correctamente, dejando un historial de aplicaciones instaladas para futuros controles.

Control de información guardada en las computadoras

Los controles son adecuados en todas las computadoras provistas por la empresa.



Resultado - Control de Recursos - Empleados

La empresa utiliza un software web para asignar tareas sus empleados y medir el progreso de un determinado objetivo o proyecto.

Cada empleado está capacitado para operar con dicho software para conocer qué tareas le corresponde y marcarlas en progreso o completadas.

Se decidió analizar los reportes del software de algunos objetivos de la empresa.



Resultado - Control de Recursos - Empleados

Se encontraron varias tareas que no habían cumplido el tiempo límite para lograrlas.

Para refinar los resultados se optó por relevar logs físicos sobre dichas tareas.

Estos logs determinaron que las tareas habían sido cumplidas por empleados que no estaban asignados a ellas.

Determinamos que la iniciativa de utilizar un software para control de recursos puede ser efectiva solo si los empleados la utilizan correctamente.

Consideramos su efectividad como **media**.



Resultado - Control de utilización de recursos - Empleados

La empresa realiza periódicamente un seguimiento de los recursos asignados a los empleados, analizando la utilización adecuada de estos.

Para ello, cada computadora/dispositivo móvil entregado por la empresa a sus empleados cuenta con un software para trackear la utilización de las aplicaciones por hora. Los informes son enviados periódicamente al servidor de la empresa.

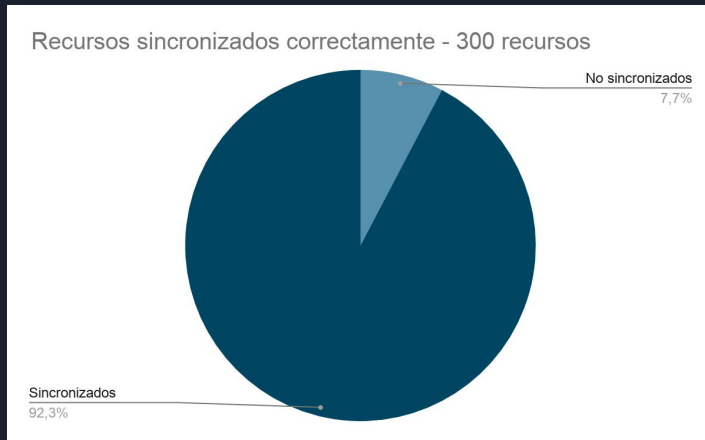
Se decidió analizar los registros en el servidor de la empresa y se encontró que ciertos recursos que se encuentra asignados (activos) no presentaban ningún registro de horas.

Resultado - Control de utilización de recursos - Empleados

Debido a las inconsistencias en los registros se decidió hacer un chequeo físico de algunos de los recursos asignados.

Se descubrió que las horas estaban siendo cargadas por el software de tracking pero que por problemas de conectividad los registros no se sincronizaban con el servidor.

Consideramos que el control de utilización de recursos podría mejorarse y determinamos su efectividad como **media**.



Control de Backups

Se le consultó a la gerencia si se realizan backups, dónde se guardan, qué seguridad tiene, quiénes tienen acceso, cuánto tiempo se almacenan, con qué frecuencia se realizan y si se realizan análisis de integridad periódicos.



Ante el descubrimiento de ambigüedades en la respuesta por parte de la gerencia, se decidió hacer un análisis más exhaustivo con los técnicos a cargo de los backups, un equipo de 5 personas que trabajan en un área de servidores. A priori sólo ellos tienen acceso a manipular y ver los backups.



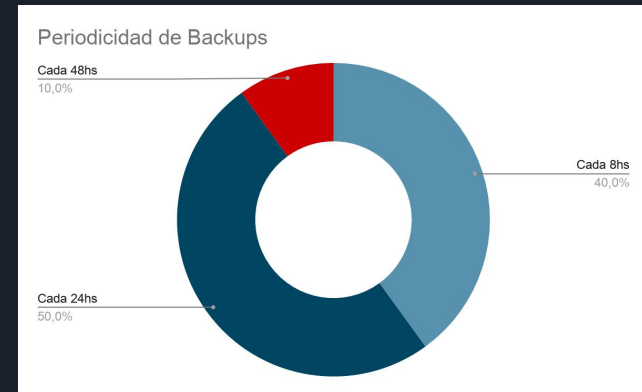
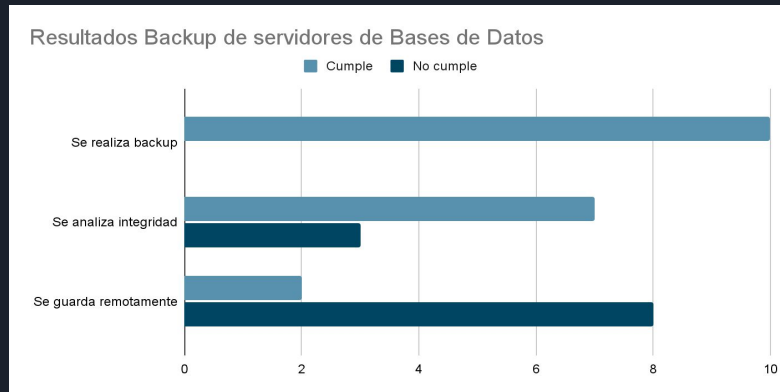


Control de Backups - Resultados

- Hay un área de administración de servidores que se encarga de supervisar el correcto funcionamiento del esquema de backups una vez por semana. La seguridad está basada en limitar los usuarios de escritura de esos backups a solo esos 5 empleados.
- Los Backups se almacenan por 10 días, luego se sobrescriben.
- Se los entrevistó para evaluar el acceso restringido a estos backups. Se decidió no confiar y se procedió a revisar los logs de acceso a los backups
- Se encontró que algunos desarrolladores también acceden a los backups sin conocimiento del equipo de servidores

Control de Backups - Resultados

- Se realiza un backup espejando el server que virtualiza los Fileservers de los archivos estratégicos para la organización en otro server pero este último se encuentra físicamente dentro del mismo datacenter.
- Por otro lado, la empresa tiene 10 sistemas de gestión que permiten llevar adelante su logística interna. Cada sistema tiene su servidores de aplicación y bases de datos de los cuales se encontró:



Resultados - Conclusión

Controles / Errores	Acceso no autorizado	Falta de logs sobre accesos de empleados	Fallos por acceso concurrente	Velocidad de red ineficiente	Caídas del sistema	Los empleados recibieron recursos que no coinciden con sus tareas	Hay empleados haciendo tareas que no le corresponde	El empleado no utiliza el recurso asignado	No se realizan backups de los servidores de Archivos y Aplicación	Errores de integridad en los backups
Control de acceso virtual	A	B								
Control de acceso físico	A	A								
Control de la red			A	A	A					
Control de recursos						B	M			
Control de utilización de recursos								M		
Control de backups	B								A	M

Efectividad: A=Alta, M=Media o B=Baja