



Gestión de Proyecto Web



GeaTech

ROL	C.I	APELLIDO	NOMBRE	E-MAIL	TEL/CEL
Coordinador	5.353.721-0	Gómez	Agustín	2agustingomez3@gmail.com	092 941 187
Subcoordinador	6.399.240-2	Domínguez	Axel	axeldq2001@gmail.com	097 213 057
Integrante 1	6.424.291-5	Sánchez	Leonardo	leoraidel11@gmail.com	097 361 149
Integrante 2	5.336.248-1	Teijeiro	Mauricio	mauriteijeiro@gmail.com	097 409 539
Integrante 3	6.416.919-9	Ramos	Andrés	andreseramos11@gmail.com	097 439 567

Docente: Gabriel Barboza

Fecha de Culminación:

9 / 09 / 2022

Segunda Entrega




Índice:

Nueva Integración al Equipo.....	2
Carta de Presentación con la nueva Integración	3
Acuse de Recibo con la nueva Integración.....	5
Ciclo de Vida del Proyecto (Reformulación).....	6
Puntos a Mejorar como Equipo.....	6
Repartición de Tareas (Asignaturas).	6
Plan de Contingencias ante riesgos.	7
Ejecución de los distintos planes de contingencia:	9
En caso de Incendio.	9
En caso de Acción de Virus Informático	13
En caso de Fallas en el Suministro Eléctrico	20
En caso de Accesos NO Autorizados	26
En caso de Robo de equipos y Archivos	30
En caso de Fallas en el Software	34
Diagramas de Planificación (Trello).	41
Diagrama de Planificación de Asignaturas:	41
Diagrama de Planificación de Requerimientos:	41
Actas de reuniones	42
Cálculo de Métricas.....	43



Nueva Integración al Equipo.


GeaTech

Carta de admisión al equipo.		
Día: 26	Mes: Julio	Año: 2022
Emitida por:		
Nombre y Apellido: Axel Dominguez	Cargo: Subordinado	

Para el Sr/Sra :

Por la presente le comunicamos que la empresa lo ha admitido como miembro del equipo de trabajo, por lo que usted debe tener en cuenta de que a partir de este momento Ud. deberá cumplir con la tareas designadas al equipo e integrarse de forma respetuosa.

Admitido,
Firma y Aclaración:
Andrés Ramos

Partes de acuerdo,
Firma y Aclaración:
Axel Dominguez
Leonardo Dominguez
Mauricio Tejera
Agustín Gómez



Carta de Presentación con la nueva Integración



GeaTech

Montevideo, 24 de Julio de 2022

Prof. Barboza, Gabriel
Gestión de Proyecto Web
Instituto Tecnológico de Informática

Presente.

A continuación los alumnos de tercero BV del turno matutino del Instituto Tecnológico de Informática nos presentamos ante usted, con el fin de informar la creación del grupo GeaTech. Los correspondientes integrantes con sus roles son los siguientes:

A continuación, se detalla dicha integración y roles del grupo:

ROL	C.I	APELLIDO	NOMBRE	E-MAIL	TEL/CEL
Coordinador	5.353.721-0	Gómez	Agustín	2agustingomez3@gmail.com	092 941 187
Subcoordinador	6.399.240-2	Domínguez	Axel	axeldq2001@gmail.com	097 213 057
Integrante 1	6.424.291-5	Sánchez	Leonardo	leoraidel11@gmail.com	097 361 149
Integrante 2	5.336.248-1	Teijeiro	Mauricio	mauriteijeiro@gmail.com	097 409 539
Integrante 3	6.416.919-9	Ramos	Andrés	andreseramos11@gmail.com	097 439 567

Por contacto al correo: geatechuy@gmail.com

Firmas:

COORDINADOR

SUBCOORDINADOR

INTEGRANTE 1

INTEGRANTE 2

INTEGRANTE 3

GeaTech

ITI

3ºBV



Gómez, Agustín

COORDINADOR



Domínguez, Axel

SUBCOORDINADOR



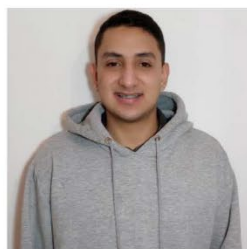
Sánchez, Leonardo

INTEGRANTE 1



Teijeiro, Mauricio

INTEGRANTE 2



Ramos, Andrés

INTEGRANTE 3

GeaTech

ITI

3ºBV



Acuse de Recibo con la nueva Integración.



Montevideo, 24 de Julio de 2022

ACUSE DE RECIBO

Corresponde a ENTREGA de Cartas de Presentación

Los alumnos de 3°BV del turno matutino, integrantes del grupo de proyecto GeaTech.

ROL	APELLIDO	NOMBRE	CI	E-MAIL	CEL/TEL
Coordinador	Gómez	Agustín	5.353.721-0	2agustingomez3@gmail.com	092 941 187
Subcoordinador	Domínguez	Axel	6.399.240-2	axeldq2001@gmail.com	097 213 057
Integrante 1	Sánchez	Leonardo	6.424.291-5	leoraidel11@gmail.com	097 361 149
Integrante 2	Teijeiro	Mauricio	5.336.248-1	mauriteijeiro@gmail.com	097 409 539
Integrante 3	Ramos	Andrés	6.416.919.-9	andreseramos11@gmail.com	097 439 567

Entregan:

Asignatura	Fecha de recepción	Firma
Análisis y Diseño de Aplicaciones Web	29/7/22	[Firma]
Formación Empresarial	6/8/22	[Firma]
Programación WEB		
Gestión de Proyectos WEB	26/7	[Firma]
Bases de Datos II	26/7	[Firma]
Sistemas Operativos III	26/7	[Firma]
Diseño Web II	27/7	[Firma]
Inglés		[Firma]
Sociología	01/08	[Firma]
Filosofía		
Dirección	26/7	[Firma]
Adscripción		
Coordinación de Informática		



Ciclo de Vida del Proyecto (Reformulación).

Puntos a Mejorar como Equipo.

- Mejorar la comunicación del grupo.
- Reunirnos más para revisar puntos del proyecto. tanto como virtualmente y presencialmente.
- Informar de todo lo necesario realizar, de lo próximo a hacer y de lo que ya está realizado.
- Comentar todo de los archivos subidos y/o borrados en las nubes, siendo estas Google Drive y GitHub.

Medios de comunicación virtual:

WhatsApp, Discord, Trello, Gmail y Crea (Plan Ceibal).

En este momento somos 5 integrantes, por lo que la repartición de tareas es más intuitiva y rápida. Además, la votación es impar, por lo que la toma decisiones, es más fácil.

Repartición de Tareas (Asignaturas).

El Coordinador y el Subcoordinador del equipo, Agustín Gómez y Axel Dominguez, son los que se encargan de la revisión de tareas faltantes, las realizadas y las necesarias de arreglos.

También hay que recalcar que los anteriormente mencionados se encuentran durante cualquier faceta en la que estemos defectuosos o tardíos.



Plan de Contingencias ante riesgos.

Descripción del problema.

A continuación, se describirán las medidas necesarias a tomar en caso de que la Cooperativa sufra algún incidente de riesgo en la cooperativa, el cual pueda afectar la sala de servidores. Este plan de contingencia está pensado para que en caso de que el servidor sufra algún percance se pueda recuperar la información lo más rápido posible y seguir trabajando.

Planificación:

Se deberá de programar en el servidor rutinas cron para que se realicen respaldos diarios de manera incremental a las 00:00 horas de:

- La base de datos en su totalidad

Si posee un servidor de repuesto ósea en “espejo” podrá hacer las copias de seguridad correspondientes para minimizar la pérdida de tiempo y ser más eficientes a la hora de establecer el sistema.

Establecer un Script para poder hacer los respaldos, según sea conveniente en su sistema, ya sea incremental o de totalidad.

- Los archivos de configuración importantes del sistema
- Los Logs importantes



También es necesario generar respaldos de manera semanal de:

- Hacer un Git push a todo el sistema con su respectivo commit para identificar el trabajo realizado y por quién fue realizado.

Y respaldos mensuales de:

- El directorio /home/ (En este se encuentran todos los scripts del sistema)

Todos estos respaldos son enviados por la red al servidor de respaldo usando Rsync.

Recursos:

En el servidor se necesitan los siguientes paquetes instalados y en funcionamiento

previo:

- crontab
- rsync
- cpio



Ejecución de los distintos planes de contingencia:

En caso de Incendio.

Evaluación, Identificación del escenario e Investigación y naturaleza de la contingencia.

En caso de incendio en la sala de servidores es de suma importancia verificar el estado en el que se encuentra el servidor, a continuación, se detallan las verificaciones previas en caso de poder ingresar a la sala.

1. Verificar el estado del servidor a nivel físico de la sala de servidores, verificar con un multímetro la fuente de poder, placa madre, y los demás componentes.
2. En caso de notar que el deterioro físico es grave fijarse en qué estado están los discos duros del sistema R.A.I.D del servidor.
3. Si alguno de los discos duros está en buen estado y da señal de vida usar el clonador de discos para respaldar la información a un disco duro externo, el cual se encuentra previsto para esto y a la nube.



4. Si nada de esto se puede realizar, se va a tener que usar el servidor de espejo o de emergencia. Luego de chequear su funcionamiento se deberá utilizar el script para recuperación llamado recuperacion.sh que se encuentra en el repositorio de GitLab de la cooperativa; Al correr este script se copiaran todos los respaldos al nuevo servidor y se hace un proceso de restauración de datos (esto puede llevar un tiempo).
5. Si nada de esto funciona la cooperativa debe encargarse de comprar nuevos equipos.

Planificación y Objetivos operativos (Precauciones para prevenir un incendio)

- Estar siempre alerta. La mejor manera de evitar los incendios, es la prevención.
- Procurar no almacenar productos inflamables.
- Cuidar que los cables de los aparatos eléctricos se encuentren en perfectas condiciones.
- No se deben realizar demasiadas conexiones en contactos múltiples, para evitar la sobre carga de los circuitos eléctricos.
- Por ningún motivo mojar las instalaciones eléctricas. Recuerde que el agua es un buen conductor de la electricidad.



- Todo contacto o interruptor debe tener siempre su tapa debidamente aislada.
- Antes de salir, la última persona en hacerlo, deberá revisar que los aparatos eléctricos estén apagados o perfectamente desconectados.
- Prohibido fumar en las instalaciones.
- Bajo ningún motivo se debe sustituir los fusibles por alambre o monedas, ni usar cordones eléctricos dañados o parchados.
- Contar con una alarma de incendios.
- Tener en un lugar visible y accesible un extintor contra incendios.
- Realizar simulacros de manera periódica.
- Debe de existir y ubicarse en un lugar de fácil acceso y visible los números telefónicos de emergencia y un botiquín.



Recomendaciones y conclusiones:

Los servidores e instalaciones de internet y servidores de aplicaciones, son de suma importancia, puesto que los mismo te permite bien sea disfrutar del servicio o almacenar una gran cantidad de información, lo que es realmente bueno, de allí la importancia de proteger servidores de incendios.

Debido a que generalmente, estos servidores poseen altas temperaturas, los mismos se encuentran en riesgo de incendio, sin embargo, se pueden prevenir accidentes.

Por eso mismo te recomendamos considerar las siguientes prestaciones para poder prevenir un desastre en el área de servidores, tener un sistema de desconexión automatizado de electricidad, sistemas de alarmas, sistemas de refrigeración efectiva, Seleccionar de forma efectiva un sistema de extinción.

Si usted no ha tomado estas consideraciones y ha ocurrido una catástrofe en el área de servidores, tome en cuenta de tener siempre un servidor “espejo” que haga los respectivos respaldos de su o sus sistemas informáticos, para proveer caída total del sistema por un tiempo muy prolongado.



En caso de Acción de Virus Informático

Evaluación, Identificación del escenario e Investigación y naturaleza de la contingencia

Tenemos que tener en cuenta sobre los problemas informáticos o virus informáticos es, tener la robustez tanto de nuestros ingenieros, para evaluar cuáles serían algunas fallas y poder proveer las mismas. Procederemos a tener documentación de los diferentes virus, para poder así proteger, sustentar y mantener los dispositivos, servidores y el sistema en sí. Para ello indagamos y probamos algunos virus, para ver cómo se podría aplicar varios planes en los que podemos ser satisfactorios con nuestro resultado.

Los diferentes virus en los cuales tenemos conocimiento y podemos tener habilidades en caso de poder resolver el inconveniente.

Tomando en cuenta que todos los virus son un mundo diferente, ya que no sabemos cómo está programado y que es capaz de ejecutar, los virus en lo que tenemos información de que hacen son:

- Troyano
- Ransomware
- Spyware
- Keyloggers
- Adware.



Para asegurar el rápido restablecimiento y un buen mantenimiento del sistema, obtuvimos la siguiente información sobre los tipos de virus:

- troyano:

Amenaza típica, se camufla como uno normal e inocente. En realidad, oculta archivos programados para tomar el control de un dispositivo.

- ransomware:

Diseñado para secuestrar ordenadores, el Atacante pide una cantidad económica a la víctima para liberar estos archivos.

- keyloggers:

Su objetivo robar datos, más concretamente averiguar contraseñas o nombres de usuario. Tiene un funcionamiento que consiste en registrar las pulsaciones de teclado que realizamos a la hora de colocar usuario y contraseña en un correo electrónico, este podrá guardar dicha información y enviarlo inmediatamente al atacante.

- Adware:

Es la amenaza más molesta para el usuario, ya que básicamente su función es inundarnos de publicidad intrusiva, las conocidas “VENTANAS EMERGENTES, BANNERS” a la hora de descargar una aplicación o navegar por la web.



Planificación y Objetivos operativos:

Presentado el problema, el gerente tendrá que evaluar si es necesario declarar el estado de "Contingencia ", en caso que se encuentre en la ejecución de un proceso crítico, si es así comunicará al personal a su cargo sobre tal hecho.

La gerencia, realizará una investigación del hecho, para detectar cómo es que los equipos de cómputo se han infectado y proponer una nueva medida preventiva para este caso; deberá hacer una evaluación general de todos los equipos de cómputo para detectar posibles amenazas de este tipo con la utilización de un antivirus como, por ejemplo: el Panda Dome; en su proceso de evaluación encontrará virus, deberá dar la opción de eliminar el virus. si es que no puede hacerlo el antivirus, recomiendan borrar el archivo, tomar nota de los archivos que se borren.

Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección. debiendo el equipo de emergencia retirarla del ingreso al sistema y poder proceder a su revisión.

Si el virus causó suficiente daño como para evitar que los equipos de cómputo operen normalmente, el gerente deberá proceder a formatear el equipo o el servidor, instalando el mismo software base y operacional al día como los backups de la base de datos.



Una vez solucionado el problema, el gerente levantará el estado de contingencia y notificará al personal involucrado.

Pruebas de Viabilidad y Medidas que se deben adoptar, aplicando los siguientes métodos o pasos, podrás tener un sistema libre de virus y te será muy viable para no perder la información vital.

Tener un plan de respaldo: respaldo de datos vitales, identificar las áreas para realizar los respaldos. (No hacer respaldos en USB: estos no están dispuestos para proteger la información, lo idóneo es tener un disco duro portátil para poder hacer los respaldos)

Tener software o aplicaciones que hagan las copias de seguridad por ti. Los equipos deben tener un antivirus instalado y actualizado. Mantener actualizado el sistema operativo y sus respectivos programas.

Establecer un Script para poder hacer los respaldos, según sea conveniente en su sistema, ya sea incremental o de totalidad. en discos duros o ya sea en un servidor aparte llamado espejo.

Si llegase a perder todos los datos de su servidor, ya al no tener disponible un servidor de respaldos o discos duros, comuníquese con su administrador de servidores para obtener otro servidor llamado “espejo”.



Solución general, ejecuto los siguientes pasos:

- Desconecte el servidor de la red para evitar que el virus se distribuya en toda la LAN, para esto puede simplemente desenchufar el cable de red.
- Utilice una aplicación antivirus para limpiar el servidor
- Restaurar los archivos por una copia de seguridad no infectada.
- Utilice nuevamente una aplicación Antivirus para asegurarse de que la restauración no esté infectada.

Antivirus disponibles para el Sistema Operativo Fedora:

- ESET NOD32
- F-Secure
- Avast Core Security
- Bitdefender Gravity Zone Business Security
- Kaspersky Endpoint Security for Linux
- McAfee VirusScan Enterprise for Linux



Se debe evitar que las licencias de antivirus expiren, se requiere renovación con anterioridad del nuevo antivirus. De lo contrario hay que buscar otra copia de seguridad.

Implicaciones financieras de las respuestas:

Tenemos que asegurarnos de que no podemos cometer el fallo de no tener una buena seguridad empresarial, para los servidores y pc en los cuales tendremos que contratar un buen sistema de seguridad Antivirus, Firewall entre otros.

Tomarse el tiempo para configurar las copias de seguridad del sistema operativo y la información de la base de datos, página web, etc. Para impedir que estos virus informáticos borren, roben y hagan de las suyas con la información de la empresa.

Si llegase a tener el poder de nuestra información, el creador del virus o el atacante nos podría pedir una suma de dinero para poder liberar la información. Algo que no debe de pasar por ninguna circunstancia porque perderíamos una cantidad de dinero significativa.



Recomendaciones y conclusiones

Las empresas deben tener en cuenta que es muy importante contar con un plan de contingencias ya que de esta manera tendrán en consideración que tanto los seres humanos como los equipos tecnológicos, somos vulnerables a sufrir riesgos de todo tipo por muy buena que sea la empresa tampoco está exenta de sufrir algún incidente. El plan de contingencia nos guía acerca de los procedimientos o pasos a seguir en caso de que ocurra algún evento. El presente plan de contingencia es una herramienta para reaccionar adecuadamente ante eventos críticos, se debe tener en cuenta una seguridad orientada a proteger todos los recursos informáticos desde un dato más simple hasta lo más valioso, la finalidad es de instruir al personal de las empresas para así tomar medidas de precaución que pueda afectar la pérdida de la información y demás recursos tecnológicos de dicha empresa.

El plan de contingencia debe ser revisado periódicamente, generalmente la revisión deberá ser consecuencia de un análisis de riesgo. Hacer de conocimiento general el contenido del presente plan de contingencia, con la finalidad de instruir al personal de la empresa y capacitar al personal de la empresa ante cualquier evento que ocurra.



En caso de Fallas en el Suministro Eléctrico

Evaluación, Identificación del escenario y la naturaleza de la contingencia

Ante un eventual corte de suministro eléctrico por parte de la empresa distribuidora, o fallas en el Sistema Interconectado Central, el Establecimiento debe contar con equipo auxiliar que permite la funcionalidad sin contratiempos y sin interrupciones en los dispositivos eléctricos, (subestación, alimentadores y tableros de distribución y líneas de iluminación y enchufes) para abastecer en los distintos servicios informáticos.

- En caso de incendio en la sala de servidores es de suma importancia verificar el estado en el que se encuentra el servidor, a continuación, se detallan las verificaciones previas en caso de poder ingresar a la sala.
- Fallo en el suministro eléctrico. Provocado por la discontinuidad en el servicio de energía eléctrica para el uso de los equipos.
- Falla total o parcial del cableado. ocasiona pérdidas totales o parciales, por lo tanto, las actividades se encuentran interrumpidas hasta solucionar el problema.



Planificación, Objetivos Generales y Específicos.

1. Verificar el estado del servidor a nivel físico de la sala de servidores, verificar con un multímetro la fuente de poder, placa madre, y los demás componentes.
 - 1.1. Si llegase a dañar algún componente del servidor, lo recomendable es tener un servidor de respaldos para no perder dinero ni tiempo a la hora de rehacer el único servidor que tiene.
 - 1.2. Si no tiene un servidor de respaldos o discos duros de respaldos, comunicarse de forma inmediata con el administrador de servidores, para obtener uno).
2. En caso de notar que el deterioro físico es grave fijarse en qué estado están los discos duros del sistema R.A.I.D del servidor.
3. Si alguno de los discos duros está en buen estado y da señal de vida usar el clon de discos para respaldar la información a un disco duro externo, el cual se encuentra previsto para esto y a la nube.
4. Si nada de esto se puede realizar, se va a tener que usar el servidor de emergencia. Luego de chequear su funcionamiento se deberá utilizar el script para recuperación llamado recuperacion.sh que se encuentra en el repositorio de GitLab de la cooperativa; Al correr este script se copiaran todos los respaldos al nuevo servidor y se hace un proceso de restauración de datos (esto puede llevar un tiempo).



5. Si nada de esto funciona la cooperativa debe encargarse de comprar nuevos equipos.

Objetivo general.

Cumplir con las condiciones necesarias relacionadas con las instalaciones para garantizar la seguridad de los usuarios.

Objetivos específicos.

Estandarizar el proceso de respuesta ante un evento de corte de energía eléctrica. Preparar al personal institucional a la respuesta ante estos eventos.

Medidas que se deben de Adoptar.

1. El funcionario debe retirar desde ubicación talleres llaves de ingreso a sector de grupo de generadores eléctricos.
2. Funcionario de turno debe dirigirse urgente al sector donde se ubica el grupo eléctrico.
3. Chequear la transferencia automática de energía desde el equipo a la red de la empresa.
4. Chequear Display de pantalla del equipo.



5. Chequear estado de luces de fallas de display.
6. Chequear parámetros de energía y de motor en Display; Voltaje, frecuencia, Presión, Rpm, Temperatura, voltaje baterías entre otros.

Investigación de la naturaleza de la contingencia.

1. Este evento incluye los siguientes elementos mínimos identificados, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Servicios Públicos:

- Suministro de Energía Eléctrica

Hardware:

- Servidores y sistema de almacenamiento de información (Storage)
- Estaciones de Trabajo
- Equipos de Comunicaciones Equipos Diversos
- UPS y generador eléctrico
- Aire acondicionado

Implicaciones financieras de las respuestas.

Si no procedemos a tener las precauciones necesarias de tener ups controladores de voltajes, entre otros, llegará a dañar algún componente de las computadoras o servidores y sería bastante caro en recuperar o comprar una fuente de poder, placa madre entre otros. Le recomendamos tomar la iniciativa



y tener un plan de contingencia presentado en tal segmento, para no tener pérdidas económicas y de tiempo en la cual después arrepentirse.

Entorno a este evento puede darse en cualquiera en las instalaciones, considerando la Sede Central y la sede donde se ubica el Centro de Datos, por tener cada una de ellas los gabinetes de comunicación y equipos que brinda servicios informáticos a los usuarios a nivel interno y externo.

El personal encargado, el/La Director/a de la Oficina de Abastecimiento y el/La Coordinador/a de Continuidad de TIC son los responsables de realizar las coordinaciones para restablecer el suministro de energía eléctrica. El Equipo de Prevención de TIC debe realizar las acciones descritas en el punto.

Condiciones de Prevención de Riesgo.

- Durante las operaciones diarias del servicio u operaciones se contará con los UPS necesarios para asegurar el suministro eléctrico en los equipos considerados como críticos.
- Equipos UPS cuentan con mantenimiento preventivo y con suficiente energía para soportar una operación continua de 30 minutos como mínimo. El tiempo variará de acuerdo a la función que cumplan los equipos UPS.
- Realización de pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.
- Capacidad de los UPS para proteger los servidores de archivos, base de datos y aplicaciones, previniendo la pérdida de datos durante las



labores. La autonomía del equipo UPS no deberá ser menor a 30 minutos.

- Disponibilidad de UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso en las instalaciones (puertas, contactos magnéticos, entre otros.)



En caso de Accesos NO Autorizados

Evaluación, Identificación del escenario e Investigación y naturaleza de la contingencia

De acuerdo al análisis de riesgos y a la revisión de seguridad realizada, se presentan las sugerencias de los casos para combatir cada uno de los riesgos potenciales a los que se enfrenta la red informática.

Según lo mostrado en la situación actual en la sección de esquema de antivirus, es necesario estandarizar el software de antivirus en todas las estaciones de trabajo y servidores. Es aconsejable tener un proveedor de software antivirus para las estaciones y otro diferente para el servidor, para reducir la probabilidad de que un virus que no esté en la lista de actualización, se filtre en toda la red. Se sugiere que en las estaciones de trabajo se siga con la línea. Puede tener instalado un Antivirus en el servidor y en la mayoría de las estaciones se encuentre instalado otro producto ya que es lo más recomendable, para la funcionalidad que brinda la consola de administración de la versión para servidores. Si no se opta por alguno se tendría que analizar que el producto que se escoja no afecte el software instalado para las actividades que realiza la empresa.



¿Por qué tener 2 antivirus diferentes, uno para el servidor y otro para las estaciones de trabajo?

Es porque estos tienen variaciones en sus tablas de definiciones de virus, es más difícil que un virus se propague por la red debido a la diversificación de productos que puedan detectarlos. Es necesario implementar un procedimiento para las actualizaciones automáticas de las definiciones de virus. Esta labor la debe realizar el administrador de red, cuidando que se ejecute en horas en que no se degrade el performance del tráfico de red.

Medidas y recomendaciones a nivel Físico.

El servidor web no debe ser accesible físicamente a cualquier Persona. Es conveniente que exista un espacio físico donde se ubique el Servidor, con acceso restringido al personal autorizado, y que cumpla con los requisitos adecuados para su funcionamiento, como temperatura ambiental adecuada, aislado del polvo y plagas dañinas. En este espacio, además de ubicar el servidor, se pueden ubicar los elementos más sensibles de la red corporativa como el HUB/Switch y el servidor proxy.

Tomar las precauciones por si llegasen a robar los componentes del servidor, tendría que obtener un servidor de respaldos para poder tener siempre esté un servidor de respaldo, para no tener pérdida de tiempo (Si no llegase tener un servidor de respaldo, comuníquese con su administrador de servidores, para tener uno lo más pronto posible).



Recomendaciones a nivel lógico.

Habilitar un firewall que evite ingresos desde redes externas hacia la Red corporativa. Para la implementación del mismo presentamos las siguientes opciones:

- Configurar adecuadamente el firewall que viene incluido con el sistema operativo Linux Fedora.
- Adquirir un hardware de seguridad que entre sus características tengan implementado un firewall, el hardware sugerido es el siguiente:
Symantec Gateway Security SGS 360 (10224331)

La recomendación de hardware incrementa los costos de seguridad, los cuales se verían justificados por la posible expansión de la empresa.

Instalar un sistema de detección de intrusos para monitorear los Accesos o tentativas de accesos a la red corporativa para esto presentamos a continuación dos opciones:

- Un software de IDS instalado en el servidor proxy de la red. Este puede ser LIDS (Linux Intrusión Detection System), que es un parche del kernel de Linux que permite implementar funcionalidades de IDS al sistema operativo, y debido a ser open source, no tiene costo.
- Utilizar el IDS que esta implementado en el Symantec Gateway Security SGS 360 (10224331).



- Deshabilitar los servicios que no sean necesarios y luego de esto verificar los posibles puertos que se encuentren abiertos innecesariamente para proceder a cerrarlos.
- Concienciar a los usuarios de la red, se deberá concienciar a los Usuarios de la red, acerca de una política mínima de seguridad, por ejemplo, evitar las claves fácilmente descifrables.
- Solo está permitido instalar en las computadoras el software requerido para el desarrollo de las actividades de la empresa, para esto se contará con un listado de dicho software, el cual deberá ser seleccionado por la Gerencia y jefes de área. Teniendo presente que la mayoría de los ataques informáticos no vienen de fuera, sino de dentro, según lo indican las estadísticas de penetración a las redes corporativas expuestas, un usuario interno podría capturar contraseñas con una herramienta Sniffer.

Para evitarlo, es conveniente que la red, en lugar de estar basada en un HUB, esté basada en conmutador (SWITCH).

Eso evitará que todos los paquetes de información lleguen a todas las tarjetas de red. Usando una red conmutada puede evitar muchos Intentos de espionaje de la información que circula por la red.

Es recomendable agregar contraseña del BIOS a todos los equipos de la red, para evitar vulnerabilidades de acceso dependientes de los Sistemas Operativos Instalados.



En caso de Robo de equipos y Archivos

Al entrar y salir de las instalaciones se deberá observar previamente que no exista ningún individuo sospechoso. Queda prohibido dar información personal de los empleados o información confidencial de la organización. Contar con personal para resguardo de las instalaciones de la empresa. Tener instalación de alarma.

Contratar pólizas de seguros, Equipos de cómputo Inventario actualizado de los equipos de manejo de información (computadoras, impresoras, etc.), especificando su contenido (software que usa) y su ubicación. Nuestra empresa podría optar por la toma de una Póliza de Seguros Comerciales como parte de la protección de los Activos Institucionales, pero haciendo la salvedad en el contrato, que, en casos de siniestros, la restitución del Computador siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.

Se deberá realizar una señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo, etiquetar (colocar un sticker) de color rojo al Servidor, color amarillo a las computadoras con Información importante o estratégica y color verde a las computadoras de contenidos normales.



Se obtendrán copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución. Para lo cual se debe contar con:

- Backups del Sistema Operativo.
- Backups del Software Base - Paquetes y/o Lenguajes de Programación.
- Backups de Productos Desarrollados (Considerando tanto los programas fuentes, como los programas objetos correspondientes)
- Backups de los Datos (Bases de Datos, Índices, y todo archivo necesario para la correcta ejecución de los Productos Desarrollados).
- Backups del Hardware, mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder continuar con las actividades para ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como ambiente y facilidades de trabajo.

Para realizar los respaldos se tendrá en consideración el uso de las herramientas de encriptación para que la información pueda ser recuperada sola y exclusivamente por quién la generó. También se recomienda tener duplicidad en los respaldos, esto es, mantener un respaldo “in situ” para mayor facilidad de recuperación, y otro respaldo fuera de las instalaciones de la empresa.



Implicaciones financieras de las respuestas.

Hardware:

Ya que, si se llegase a dañar algún componente del servidor de alguna pc o laptop, de la empresa podrían ser muy costosas a la hora de arreglar algún componente dañado. ya que estos mismos fueron hechos para soportar grandes cantidades de información, procesamiento y energía eléctrica.

Software:

A nivel de software, ya que, si se obtiene una copia de seguridad tanto como del servidor o de los dispositivos, no sería tan tedioso o costoso de hacer. Pero si no precisamos de tal respaldo podríamos tener un gran problema administrativo. procedemos a comprar los softwares necesarios y rehacer todo desde el principio.

Recomendaciones y conclusiones.

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y esforzando los elementos que funcionaron adecuadamente. El otro elemento es evaluar cuál hubiera sido el costo de no haber tenido nuestra Institución el plan de contingencias llevado a cabo.

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción y cómo se comportaron los equipos de trabajo.



De la Evaluación de resultados y del siniestro en sí, darán como resultado dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionó el siniestro.



En caso de Fallas en el Software

Evaluación, Identificación del escenario e Investigación y naturaleza de la contingencia.

Las alteraciones o complicaciones que sufran los servidores en el software pueden ser corregidas en la mayoría de los casos, sin embargo en algunas ocasiones, las alteraciones llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse hasta por días sin tener la absoluta certeza de que las correcciones que se hicieron fueron las necesarias, por tal motivo es mejor acudir a los respaldos de información y restaurar los datos, de esa forma las operaciones del día no se verán afectadas y al mismo tiempo se ponen al día los datos faltantes de la operación del día anterior.

Identificación del escenario.

Pantalla azul del sistema, bloqueos frecuentes, reinicios, velocidad de respuesta lenta

El servidor es muy similar a nuestra computadora común, ya sea una estructura de hardware o un sistema operativo. Por lo tanto, al igual que nuestra computadora, puede estar infectada con virus. También provocará fallas, pantallas azules, reinicios y otras fallas debido a vulnerabilidades del sistema, conflictos de software y fallas de hardware. También causará falta de respuesta debido a la excesiva información almacenada en caché.



Para el servidor, la estabilidad y la seguridad son la primera prioridad. Por lo tanto, solo necesitamos asegurar las funciones más básicas del servidor, así como las tarjetas de sonido están prohibidas por defecto. No necesitamos demasiadas funciones, ni necesitamos demasiada compatibilidad con puertos. Por ejemplo, algunos puertos innecesarios y riesgosos pueden ser bloqueados. Para algunos puertos necesarios y riesgosos, como los puertos 3389, 80, etc., podemos establecer puertos secretos no especificados modificando el registro, de modo que los riesgos de seguridad de los puertos del servidor ya no existan.

Otros problemas muy comunes:

Tarjeta de red del servidor, en el caso de una tarjeta general, compruebe primero el uso de su servidor.

Falla de la tarjeta de red del equipo, falla del cable de red y falla del interruptor superior. Antes de la falla, puede probar la IP adyacente de su servidor. Si la IP adyacente también tiene pérdida de paquetes, significa que el equipo de conmutación de la capa superior está defectuoso.

Si la tasa de uso de la CPU es superior al 50% y si el uso de memoria es demasiado alto.



Si en caso de que su servidor este con un consumo excesivo de CPU o de RAM proceda con lo siguiente:

- Reiniciar el ordenador.
- Finalizar o reiniciar procesos

Para finalizar los procesos en su servidor Linux pruebe con los siguientes comandos:

- Kill: matar un proceso usando su PID.

La forma más complicada, pero al mismo tiempo más precisa de matar un proceso es a través de su PID (siglas en inglés de «Identificador de Proceso»).

Cualquiera de estas 3 variantes puede servir:

- kill -TERM pid
- kill -SIGTERM pid
- kill -15 pid
- killall - matar un proceso usando su nombre.

Un dato a tener en cuenta al usar este método es que en caso de que haya más de una instancia de ese programa ejecutándose, se cerrarán todas.

- killall nombre_proceso
- pkill - matar un proceso usando parte de su nombre.



Es posible aniquilar un proceso especificando el nombre completo o parte del nombre. Eso significa que no hay necesidad de que recuerdes el PID del proceso para enviar la señal.

- pkill parte_nombre_proceso
- xkill - matar un proceso seleccionando la ventana con el mouse.

Este es el método más sencillo y el más práctico. En caso de desastre, simplemente presiona Alt + F2 para que se abra el cuadro de diálogo que te permitirá ejecutar comandos. Desde allí, ejecuta el siguiente comando:

- xkill

El cursor del mouse se transformará en una pequeña calavera. Todo lo que resta es hacer clic en la ventana que quieres cerrar y listo. Chau proceso.

Si se produce la situación anterior, significa que su servidor o red no puede llevar su servicio actual. Póngase en contacto con el personal técnico para ajustar sus recursos.

Objetivos.

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.



Planificación, ejecución y Objetivos.

Es necesario siempre la revisión exhaustiva de cada uno de los componentes que conforman nuestro sistema, por ello, debemos realizar una etapa de diagnóstico para poder asegurar que las acciones de solución propuestas tengan un fundamento realista y no tener que volver a rehacer toda propuesta

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.
- Insertar un servidor espejo y discos duros para hacer el respaldo de los diferentes archivos.

En caso de que la alteración haga imposible el inicio inmediato de las operaciones se procede como se indica de la siguiente forma:

- Recoger los respaldos de datos, programas, manuales y claves del lugar en el que se encuentran los resguardos.
- Si las fallas se derivan del mal funcionamiento de un equipo (Hardware) se procede a su reemplazo inmediato o remitir a la póliza de mantenimiento.
- Instalar el sistema operativo.
- Restaurar la información de la base de datos y programas.



- Revisar y probar la integridad de los datos
- Iniciar las operaciones

En caso en que las alteraciones puedan ser corregidas sin problemas tan graves, procederemos conforme a lo siguiente:

- Corrección de las alteraciones que se localicen en los servidores hardware.
- Corrección de las alteraciones que se localicen en los servidores software.
- Revisar y probar la integridad de los datos
- Iniciar las operaciones

Implicaciones financieras de las respuestas.

Hardware:

Ya que, si se llegase a dañar algún componente del servidor de alguna pc o laptop, de la empresa podrían ser muy costosas a la hora de arreglar algún componente dañado. ya que estos mismos fueron hechos para soportar grandes cantidades de información, procesamiento y energía eléctrica.



Software:

A nivel de software, ya que, si se obtiene una copia de seguridad tanto como del servidor o de los dispositivos, no sería tan tedioso o costoso de hacer. Pero si no precisamos de tal respaldo podríamos tener un gran problema administrativo. procedemos a comprar los softwares necesarios y rehacer todo desde el principio. No sería tan costoso reparar

Recomendaciones y conclusiones.

En este plan de contingencia, podemos asegurar que hemos indagado e informado sobre el tema. Podemos asegurarnos de que el plan seleccionado es el mejor y el más competente, para asegurarnos de que sea lo más eficiente y sin complicaciones a la hora de llevarlo a cabo.

Ya que se tiene una evaluación de riesgos, y se han identificado las amenazas potenciales a la infraestructura de TI, el siguiente paso será determinar qué elementos de dicha infraestructura son los más importantes para las operaciones corporativas. Asumiendo que todos los sistemas y redes TI funcionan con normalidad, la empresa debería ser plenamente viable, competitiva y sólida desde el punto de vista financiero.

Un porcentaje muy alto de los incumplimientos de los acuerdos a nivel del servicio en proyectos de TI es debido a la caída de infraestructura Hardware o Software, en este caso la cual supone una afectación en el servicio software sin previo aviso. De forma proactiva se establecen planes y herramientas que mejoren la capacidad del entorno, pero de forma reactiva, están los llamados Planes de Contingencia para tecnologías de la información (TI).



Diagramas de Planificación (Trello).

Diagrama de Planificación de Asignaturas:

<https://trello.com/b/leWpGGVJ/kanban-asignaturas>

Diagrama de Planificación de Requerimientos:

<https://trello.com/b/7GyV0gRT/kanban-requerimiento-de-software>



Actas de reuniones

Enlace de la carpeta de las Actas de reuniones:

<https://drive.google.com/drive/folders/1fH1TD6XoeieSEEtyrYogZoZpGd2Kqkb6?usp=sharing>



Cálculo de Métricas

Enlace de la carpeta de las Métricas y las fotos del sistema:

https://drive.google.com/drive/folders/1kfb8D-aEgy-WZk9a_jAJs1qpemeVoXI7?usp=sharing