**Asignatura:** Seguridad y Auditoría Informática

**Sección:** 371

**Nombre del docente:** Leighton Torres Carlos Alberto

**Nombre de los integrantes del grupo:** Ivo Olivares, Felipe Inda, Yerko Fuentes.

**Fecha de entrega:** 7 de mayo de 2019

BLUE TEAM

Herramientas, Planes y Políticas

de Seguridad

Empresa JetBlack LTDA.

Contenido

[I. Introducción. 3](#_Toc8651957)

[II. Políticas de Seguridad. 4](#_Toc8651958)

[III. Definición perfiles, responsables y sanciones. 8](#_Toc8651959)

[IV. Definición Planes de Contingencia y Continuidad Operativa. 8](#_Toc8651960)

[V. Material de Concientización para los Usuarios Finales. 11](#_Toc8651961)

[VI. Planificación del Procedimiento de Actualización. 15](#_Toc8651962)

[VII. Publicación y divulgación de las Políticas a la Organización. 21](#_Toc8651963)

[VIII. Conclusión 22](#_Toc8651964)

[IX. Referencias bibliográficas 23](#_Toc8651965)

1. Introducción.

A continuación, se procederá a realizar un levantamiento de infraestructura TI en lo relacionado a seguridad informática, considerando planes de informática y continuidad del negocio.

En este aspecto, es importante hablar del usuario del sistema que se desarrollara ya que, **en términos de vulnerabilidad, es quien acumula mas vectores posibles de ataque**, a nivel de experticia con los equipos, como permitir la entrada de malware por desconocimiento, puede ser a través de dispositivos móviles o correos electrónicos, de forma accidental o intencional, también a nivel de **ingeniería social**, la cual consiste en la interacción social que busca obtener beneficios de un usuario de cierto sistema, el cual entrega información confidencia o proporciona los medios para obtenerla.

El trabajo por realizar consiste en minimizar las posibilidades de ataque, en el ámbito social, físico y lógico, y en el caso de concurrencias identificadas como ataque o perdida, contar con los medios, procedimientos y personas necesarias para paliar la situación.

La empresa JetBlack, quien ya ha recibido un análisis por parte de los alumnos INACAP desea estructurar sus procesos e infraestructura TI de manera que la seguridad quede cubierta, considerando los principales vectores de ataque utilizados por los cibercriminales.

El plan para lograr estos objetivos, en esta ocasión, abarca:

**1- Políticas de seguridad.** Se trata de un plan de distintas actividades enfocado, en primera instancia, a evitar, detener y mitigar las situaciones de criminalidad y desastres.

**2- Perfiles y responsabilidades.** De esta manera cada trabajador es capaz de operar sus actividades con menor supervisión a la esperada en una empresa sin estructura, además de saber sus obligaciones y libertades sin mayor trabajo.

**3- Planes de contingencia y continuidad operacional.** Consiste en preparar a la organización para estado de problemas en el ámbito de la infraestructura empresarial critica para que el negocio opere durante los tiempos acordes previamente pactados con los clientes.

**4- Material de concientización para el usuario final.** Son consejos del departamento de informática que buscan resguardar la información que exponen de manera natural los usuarios finales, para que esto no suceda se recomiendan ciertas buenas practicas a la hora de utilizar y almacenar dispositivos.

**5- Planificación del proceso de actualización.** Consiste en mantener un plan con documentación sobre las fases de la implementación en infraestructura, en este caso tecnológica, con el fin de poder revisar los cambios entre versiones, mejoras, descartes, requisitos y otras características de producción.

**6- Publicación y divulgación de las políticas organizacionales.** Identifica los factores comunicacionales que interfieren en la comunicación de las políticas de organización a los trabajadores, ejecutando las maniobras adecuadas para dar a conocer la información relevante para los actores.

1. Políticas de Seguridad.

En este apartado se da a conocer las políticas de seguridad de cada área de la empresa JetBlack, para ellos debemos conocer que son las políticas de seguridad y cual es su enfoque principal.

Las políticas de seguridad son un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa. Se trata de una especie de plan realizado para combatir todos los riesgos a los que está expuesta la empresa en el mundo digital. De esta forma mantendremos nuestra organización alejada de cualquier ataque externo peligroso. (SEK, 2009)

En la actualidad existe una gran cantidad de ciberdelincuencia que apuesta por atacar a las empresas de sus aparatos informáticos para conseguir información valiosa que pueda permitirles realizar estafas o sacar algún beneficio. Con la transformación digital que han sufrido las empresas actuales, es necesario controlar mucho más todos los aspectos relacionados con la tecnología, ya que cualquier error puede provocarnos grandes problemas.

También es necesario establecer cuáles son los mecanismos de seguridad que vamos a implantar en nuestra empresa. Estos tendrán que plantearse en tres ámbitos de actuación diferentes:

* **Prevención.** Recuerda que más vale prevenir que curar, por lo que esta primera fase será imprescindible para no tener problemas.
* **Detección.** En el caso de tener alguna amenaza será necesario saber cómo detectar y realizar diagnósticos adecuados sobre los errores recibidos.
* **Actuación.** Por último, en el caso de que se produzca alguna inviolabilidad de nuestro sistema informático es necesario establecer protocolos de actuación que nos permitan solucionar cualquier amenaza de la forma más rápida y efectiva posible.

1. **Políticas del Áreas de Desarrollo.**

Las políticas que se aplican en esta área son las siguientes.

1. Diariamente se realizan Backups automáticos a la base de datos según los mecanismos establecidos y se realizan a cada hora.
2. Los equipos deberán contar con salvapantallas protegido por contraseña con un tiempo de espera de 1 minuto para evitar accesos no autorizados.
3. Todos los accesos a los programas principales estarán protegidos mediante un mecanismo de usuario y contraseña, así como permisos de acceso. De igual forma, las sesiones de Windows personales estarán protegidas con contraseña.
4. Los usuarios deberán abstenerse de divulgar o compartir sus datos de acceso a los programas y sesiones de Windows.
5. Coordinación o sistemas designarán periódicamente nuevas contraseñas tanto para el acceso a las sesiones Windows como para el acceso a los programas.
6. Todos los archivos que viajen por correo y que contengan información sensible deberán estar comprimidos con contraseña de uso interno como medida de seguridad de información.
7. Todos los equipos asignados a los conectores/gestores tendrán deshabilitados los accesos a puertos USB, CD o Diskettes.
8. Los equipos autorizados para el uso de dispositivos de almacenamiento externos están supervisados por coordinación y por el área de sistemas, para la entrada y salida de información.
9. A todos los equipos se les realizará una revisión de virus por lo menos cada mes.
10. Cuando lo considere necesario, cualquier miembro del Grupo de coordinación podrá solicitar al Administrador del proyecto la celebración de una reunión adicional del grupo para la atención de asuntos relativos al Proyecto de desarrollo.
11. **Políticas del Área de Sistemas y Soporte.**
12. Todos los equipos deberán presentar las últimas actualizaciones de Windows, parches de seguridad y antivirus instalado.
13. Los equipos de toda la agencia deberán de estar conectados a un regulador de corriente, como medida de prevención de variaciones de electricidad.
14. Si se presentara una suspensión de servicio eléctrico y el servidor solo se sostuviera con el no-break, se tendrán que apagar primero todos los equipos de la agencia y posteriormente el servidor.
15. El servidor y la máquina principal del área administrativa deberán conectarse a un equipo no-break para evitar la pérdida de información en los equipos por variaciones o fallas de energías.
16. Una vez al año se realizará una revisión en la red para detectar desperfectos y dar así mantenimiento a la agencia.
17. Periódicamente, por espacio de 4 meses, se realizará una limpieza física a toda la infraestructura de equipo de cómputo por parte del personal de sistemas.
18. Toda actividad elaborada por el equipo de sistemas deberá de estar debidamente documentada para darle seguimiento y que sirva como evidencia en los procesos de auditoria interna.
19. El proceso de construcción y/o mantención de sistemas de información, debe contar con normas de programación, personamiento, documentación y pruebas para cada etapa del ciclo de vida: construcción, pruebas, explotación.
20. Toda la documentación asociada al ciclo de construcción y/o mantención de sistemas de información debe tener procedimientos de control de personamiento.
21. Se prohíbe el uso y/o copia de cualquier paquete de software, por parte de los funcionarios, del cual no se disponga de su respectiva licencia que lo autorice.
22. **Políticas del Usuarios Finales.**
23. Cada empleado tiene establecido un equipo de cómputo al cual debe ingresar con un usuario y contraseña.
24. El personal debe hacer uso adecuado de los recursos informáticos (PC, impresoras, programas, correo, etc.) y el personal de sistemas debe asegurar que se cumpla esta política. Además, todo el personal deberá informar a sistemas sobre cualquier falla, desperfecto o mal uso del equipo de cómputo, para su adecuado seguimiento.
25. Todo el personal tendrá una cuenta de correo electrónico interno, que les permite recibir y enviar información indispensable para sus actividades. Estas cuentas de correo sólo son para uso interno, no tienen la capacidad de enviar correos públicos.
26. El uso de internet queda reservado solo para las actividades de trabajo que así lo requieran. En general se restringe el acceso mediante el uso de contraseña en el administrador de contenidos de Internet Explorer.
27. Se prohíbe a los usuarios dar a conocer a terceras personas su contraseña, quien así lo hiciere debe tomar en cuenta que sigue siendo el único responsable de las actividades que se realicen con su identificación de usuario (ID) y contraseña.
28. El usuario debe asegurarse que al digitar su contraseña no esté siendo observado por ninguna persona.
29. Se prohíbe introducir en los computadores personales cualquier tipo de medio de almacenamiento sin que previamente haya sido revisado para descartar la presencia de virus o cualquier otro programa dañino.
30. El usuario deberá abstenerse de abrir o reenviar mensajes de correo electrónico que no provengan de fuentes conocidas y seguras, y de descargar anexos enviados por correo electrónico que puedan ser fuente de virus o similares o cuya procedencia y características desconozca.
31. En caso de pérdida del computador personal, se debe reportar de inmediato.
32. Los computadores de escritorio deben ser apagados una vez terminada la jornada de trabajo y dejar la oficina con las debidas seguridades de accesos.
33. **Políticas del Área de Gestión.**
34. Gestionar el desarrollo de los sistemas informáticos de la Subsecretaría, tanto para los desarrollos propios o externalizados.
35. Supervisar el desarrollo de sistemas por parte de proveedores de servicios.
36. Administrar los sistemas productivos de la Subsecretaría y mantener la operatividad de los sitios WEB Institucionales.
37. Detectar, diseñar e implementar mejoras en los sistemas de gestión interna.
38. Revisión permanente de nuevas tecnologías que permitan mejorar las soluciones ya existentes.
39. Los dueños de la información serán los responsables de verificar que existan procedimientos y procesos de Seguridad para asegurar el manejo y la integridad de la información que reside en medios magnéticos o en documentos.
40. Se debe aplicar estándares y buenas prácticas sobre manejo de un modelo seguro de datos.
41. Todos los empleados que manejen información sensible de la Compañía deberán firmar un acuerdo de confidencialidad.
42. Todos los contratos para los nuevos empleados deben incluir una cláusula de confidencialidad.
43. Respecto al manejo de documentos, la empresa dispone que toda la información deberá estar clasificada por niveles de seguridad acorde al contenido siguiendo la codificación establecida por la empresa.
44. Definición perfiles, responsables y sanciones.

Los incumplimientos de las obligaciones empresariales en materia laboral generan distintos tipos de responsabilidades jurídicas, cada una de las cuales cumple una diferente función.

* **La Sanción penal**. Es la que se reserva a las conductas de los ciudadanos que se considera que atentan de manera más grave contra la convivencia pacífica, poniéndola incluso en peligro.
* **La Responsabilidad administrativa.** Sus características parecidas a la penal, sin embargo, implica un grado de reproche menor y por lo tanto, en teoría, una sanción menos dura.
* **La Responsabilidad civil.** Es esencialmente distinta de las dos anteriores, ya que no busca la reparación del daño hecho a la sociedad, sino la indemnización de las personas que han sido directamente perjudicadas por una conducta ilícita

|  |  |  |  |
| --- | --- | --- | --- |
| **Tipificación de infracciones** | | | |
| **Incumplimientos** | **Infraccionas Leves** | **Infracciones Graves** | **Infracciones muy Graves** |
| Normas de prevención general | X | X | X |
| Notificación de apertura | X | X | - |
| Confidencialidad de los datos Empresariales | X | X | - |
| Registro y archivo de documentación | - | X | - |
| Ordenación interempresarial | - | X | - |
| Formación/información a trabajadores/as | - | - | X |
| Formación y asignación de recursos a los delegados/as de Prevención | - | X | - |
| Servicio de Prevención | X | X | - |

1. Definición Planes de Contingencia y Continuidad Operativa.

En este apartado se detallará de forma breve y sencilla cuales son las operaciones por realizar en caso de que ocurra un incidente de forma intencional, natural o planeada a los activos importantes de la empresa y retomar las actividades lo más rápido posible.

1. **Desastres Naturales.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | 1. Incendio | | | **Impacto** | * Pérdida de información parcial o total. * Zona de trabajo inutilizable. * Gastos adicionales para su restauración. | | **Áreas afectadas** | Zona inicial de propagación que puede llegar a toda la empresa. | | **Forma(s) de Mitigación** | * Extintores. * Detectores de Humo. * Salidas de emergencia. | | **Líder Responsable** | Jefe del área afectada. | | **Plan de Respaldo** | * Revisión de extintores y detectores de humos. * Realización de copias de respaldo de la información y traslado a otra ubicación. * Implementación de Simulacros. | | **Plan de Emergencia** | * Evacuación inmediata mediante las salidas de emergencia. * Mitigación de la zona de inicio del incendio. | | **Plan de Recuperación** | * Cálculo de pérdidas. * Costos de Reposición. * Restauración de copias de seguridad. | | |  |  | | --- | --- | | 1. Corte Eléctrico | | | **Impacto** | * Pérdida de información sin respaldar. * Retraso de las actividades habituales. * Generación de incendio. | | **Áreas afectadas** | Zona afectada o toda la empresa. | | **Forma(s) de Mitigación** | * Generadores Eléctricos. * Ubicación Externa. | | **Líder Responsable** | Jefe del área de soporte | | **Plan de Respaldo** | * Revisar y recargar generadores. * Compra de nuevos generadores. * Revisión de sistema eléctrico. * Realizar copias de seguridad de la información. | | **Plan de Emergencia** | * Activación de generadores. * Traslado a ubicación de respaldo total. | | **Plan de Recuperación** | * Levantamiento del suministro de energía. * Regreso a ubicación original. | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | 1. Terremoto | | | **Impacto** | * Destrucción parcial o total del establecimiento. * Paralización de las actividades empresariales. * Gastos adicionales para reconstrucción. | | **Áreas afectadas** | Todo el establecimiento | | **Forma(s) de Mitigación** | * Operaciones Daisy. * Salidas de Emergencias. * Ubicación Externa. | | **Líder Responsable** | Todo el personal dentro de la empresa | | **Plan de Respaldo** | * Evaluación de zona alternativa de trabajo. * Verificación de las zonas seguras establecidas. * Prácticas de simulacro. * Envío de documentación sobre cómo actuar. | | **Plan de Emergencia** | * Mantener la calma en el lugar que se encuentra. * Evacuar a zonas de seguridad marcadas de forma segura. | | **Plan de Recuperación** | * Regreso seguro a la empresa. * Revisar sectores dañados o destruidos. * Calcular costos de reparación. | | |  |  | | --- | --- | | 1. Inundaciones | | | **Impacto** | * Pérdida de información física y/o digital. * Obsolescencia de instrumentos de trabajo. * Inutilización de zona de trabajo. | | **Áreas afectadas** | Zona afectada | | **Forma(s) de Mitigación** | * Copias de Seguridad. * Mantención de la infraestructura. * Ubicación Externa y/o alternativa. | | **Líder Responsable** | Jefe del área de mantenimiento y soporte | | **Plan de Respaldo** | * Limpieza constante de canaletas y reparación de entretecho. * Realización de copias de respaldo de la información y traslado a otra ubicación. * Evaluación de zona alternativa y externa. | | **Plan de Emergencia** | * Reparación inmediata de la zona de filtrado. * Traslado a ubicación externa o alternativa. * Realización de copia de seguridad. | | **Plan de Recuperación** | * Análisis de los daños * Retorno a ubicación original * Reposición del nuevo instrumento de trabajo | |  |  | |

1. **Robo de Información.**

|  |  |
| --- | --- |
| **Impacto** | * Ventas de información secreta y confidencial a otras empresas o personas externas * Exposición de información secreta importante * Pérdida de clientes y proveedores |
| **Áreas afectadas** | Áreas con información sensible |
| **Forma(s) de Mitigación** | * Copias de Seguridad * Encriptación de archivos * Seguimiento de movimientos (rastreo del empleado) * Cámaras de seguridad |
| **Líder Responsable** | Jefe del área de TI |
| **Plan de Respaldo** | * Realización de copias de seguridad y traslado a otra ubicación constantemente * Instalación de cámaras de seguridad * Encriptación de la información sensible |
| **Plan de Emergencia** | * Revisión de grabaciones de las cámaras. * Análisis de los movimientos de(los) empleados(s) sospechosos. |
| **Plan de Recuperación** | * Recuperación de copias de respaldo. * Bloqueo de acceso a(los) sospechoso(s) a la zona de trabajo. * Notificación de despido. |

1. **Destrucción parcial o total de Software y Hardware.**

|  |  |
| --- | --- |
| **Impacto** | * Inutilización del material de trabajo * Retraso en la realización de las actividades * Pérdidas de ganancias |
| **Áreas afectadas** | Áreas donde se manipula la información |
| **Forma(s) de Mitigación** | * Cámaras de seguridad * Políticas de Usuarios * Creaciones de Back-ups |
| **Líder Responsable** | Jefe del área de TI |
| **Plan de Respaldo** | * Implementación de Back-Ups y creación de ellas cada 2 semanas * Creación de políticas de seguridad en cada zona de trabajo |
| **Plan de Emergencia** | * Reemplazo del software dañado o destruido * Corrección del hardware eliminado o infectado mediante back-ups * Revisión de grabaciones de las cámaras |
| **Plan de Recuperación** | * Levantamiento y funcionamiento del nuevo software * Creación de nuevo back-up para el hardware instalado |

1. **Suplantación de Identidad**

|  |  |
| --- | --- |
| **Impacto** | * Infección al controlador central de la empresa * Falsificación de datos de forma digital y física * Adulteración de datos almacenados * Robo de información |
| **Áreas afectadas** | Toda la empresa |
| **Forma(s) de Mitigación** | * Usuario y Contraseña con especificaciones y personal * Kit de concientización |
| **Líder Responsable** | Jefe del área de TI |
| **Plan de Respaldo** | * Cambios de contraseña constante * Verificación de inicio de sesión * Concientización sobre correo y páginas no deseadas |
| **Plan de Emergencia** | * Captura de pantalla del correo recibido * Imprimir captura realizada como respaldo * Notificar al área de TI de lo ocurrido * Bloquear cuenta afectada inmediatamente |
| **Plan de Recuperación** | * Configuración de las cuentas y políticas de la empresa * Reuniones sobre capacitación |

1. Material de Concientización para los Usuarios Finales.

En este punto se hablará de la conducta que deberán tener los trabajadores de la empresa, así como el uso de diferentes artefactos electrónicos y de qué forma se establecerá que estos conocimientos sean aprendidos y verificados. (Cesar Farro, 2018)

1. **Uso de Dispositivos Electrónicos.**
2. **Celulares.** Todo uso de celulares dentro de la empresa está permitido, pero será de su responsabilidad el resguardo de este; en caso de pérdida la empresa no se hace cargo de reponerlo. Su uso solamente será de carácter informativo, evite la procrastinación en horas de trabajo. Utilice protección con cifrado ***(clave PIN, huella digital, patrón de dibujo, entre otros)*** para evitar que otros trabajadores o personas externas tengan acceso a su dispositivo. Configure VPN si se conecta en otras redes que no son de la empresa para evitar pérdidas de datos.
3. **USB, Tarjeta de Memoria, CD/DVD.** Estos dispositivos solamente pueden ser usado como almacenamiento de archivos de su trabajo realizado solamente en caso de emergencia, está prohibido transferir datos de carácter importante y confidencial de la empresa, además de la instalación de programas que no corresponden a las actividades diarias. Es responsabilidad del propietario de su resguardo, en caso de pérdida la empresa no responde por un reemplazo y todo archivo guardado deberá de realizarlo con encriptación para que otros no puedan acceder a ella.
4. **Datos Personales.**
5. **Usuario y Contraseña.** Los empleados de la empresa para acceder al ambiente de trabajo deberán de ingresar su usuario y contraseña personales, es decir, no pueden ser compartidas con otros trabajadores ni con personas del exterior. La contraseña se restablecerá cada mes para asegurar la seguridad de la empresa y evitar que el trabajador memorice la misma contraseña además de tener ciertos requisitos a la hora de crearla ***(deberá poseer al menos 8 caracteres, uso de mayúsculas, minúsculas y números, evitar usar datos sensibles y/o privados a la hora de crearla, entre otros)***, en caso de olvidarse deberá ir al área de TI para que desbloque su cuenta y escriba una nueva contraseña.
6. **Correo Electrónico.** Todos los trabajadores tendrán a disposición de un correo electrónico de trabajo que será el medio principal en donde se transmitirá los comunicados oficiales de la empresa, al igual que el usuario y contraseña es de carácter personal y único, no puede ser usado por otros ni por personas externas de la empresa. Evite ingresar a enlaces de dudosa procedencia, verifique que el destinatario sea correcto y revise la ortografía del documento.
7. **Información de la Empresa.**
8. **Datos Confidenciales.** Toda información que se trabaja dentro de la empresa es de carácter confidencial y la información de mayor relevancia será de carácter secreta. Estos datos no deben ser compartidos a ninguna persona externa u otra empresa, en caso de revelarse y verificado que se ha compartido esta información, se le bloqueará todo acceso a su zona de trabajo y será notificado inmediatamente de su despido.
9. **Utilización del Nombre de la Empresa.** Toda información en donde se requiera utilizar el nombre de la empresa debe ser usada de tal forma en que no sea perjudicial y no manche la reputación, valores e imagen que representa.
10. **Documentación.**
11. **Distribución.** La información de trabajo será transmitida mediante reuniones programadas y por el correo de la empresa, toda información que se les transmita que no sea por las vías anteriores mencionadas, deberá de tener precaución y verificar que sea correcta, de lo contrario, ignorarla por completo y seguir con su labor habitual.
12. **Copia de Seguridad.** La empresa realizará copias de seguridad a todos los archivos enviados y recibidos mediante el correo electrónico al finalizar las horas laborales, logrando una mayor seguridad de la información, por lo cual, está prohibido entrar a la zona de los servidores a todo trabajador que no esté autorizado para su ingreso, además contará con cámaras de seguridad y entrada con contraseña para vigilar el ingreso al sector y corroborar que el trabajador corresponde al que tiene los privilegios.
13. **Destrucción Segura.** Todo dispositivo, archivo o sistema de almacenamiento que será destruido, deberá de realizarse de forma segura mediante los mecanismos correspondientes instalados en la empresa. Si se desea eliminar un documento físico, este se realizará mediante una trituradora y deberá de hacerlo 2 veces, si se trata de sistemas de almacenamiento y/o dispositivo primeramente se formatea de forma segura para eliminar todos los archivos guardados y después destruirlo logrando impedir su correcto funcionamiento o restauración aun si se llega a instalar en otro computador, esto permitirá no dejar evidencia debido a que si solo se llega a formatear, la información se puede recuperar de múltiples formas.
14. **Software y Hardware.**
15. **Sistema Operativo.** El sistema operativo que se usará en la empresa será uno predefinido por el área de informática, por lo cual, el trabajador deberá de tener un conocimiento general de dicho sistema operativo y que sabe el funcionamiento de la gran mayoría del software lanzado. Todos los programas por utilizarse serán licencias oficiales y en caso de pérdida y/o eliminación del programa, la nueva licencia será pagada con el sueldo del trabajador que realizó esta acción.
16. **Tecnología en General.** Cualquier daño hecho a las tecnologías que están instaladas y distribuidas en la empresa, será responsabilidad del causante que deberá de reponer a la brevedad el dispositivo dañado y funcione correctamente. El plazo máximo que tiene para reemplazarlo será de 3 días hábiles contando el día de su destrucción o malfuncionamiento.
17. **Programas de Terceros.** Está sumamente prohibido la instalación de programas que no corresponde a lo establecido por la empresa ya sea por medios físicos ***(CD, DVD, USB, Discos Duros, tarjetas de memoria, entre otros medios)*** como por internet ***(véase páginas web, correo electrónico)***. Los programas que serán utilizados dentro de la empresa y en las zonas de trabajo serán instalados mediante políticas por el área de informática.
18. **Hábitos o Conductas.**
19. **Dentro de la empresa.** Todo trabajador deberá de tener una conducta en base a los valores que entrega la empresa; vestimenta formal, evitar confrontamientos en horas de trabajo y respetar las opiniones de los otros empleados. No se puede comer en horas de trabajo, para ello está el bloque de almuerzo. Está sumamente prohibido el consumo de bebidas alcohólicas y tabaco tanto dentro como en las cercanías de la empresa, incluso durante el bloque de almuerzo, con ello creará un mejor ambiente de trabajo.
20. **Horarios.** Cada trabajador debe de cumplir con los horarios establecidos de entrada y salida correspondiente, los horarios de almuerzo y horarios de reuniones. Si el trabajador se ausenta deberá de notificarlo a la brevedad en el correo de la empresa, indicando las razones y acoplando una copia de la licencia médica verídica. De lo contrario, el trabajador deberá de cumplir horas extras para completar las faltantes además de una advertencia correspondiente en donde se indicará qué si sigue con esta irresponsabilidad, será despedido y desvinculado de todas cuentas de la empresa.
21. **Formas de Capacitación.**
22. **Reuniones.** Cada fin de mes se seleccionarán trabajadores al azar que realizarán un pequeño cuestionario que verificará que conocen estas políticas, de aprobarlo firmarán y admitirán que conoce y ha leído sobre esto, de lo contrario deberán de quedarse y volver a leer el documento correspondiente el cual será controlado por un personal de la empresa, una vez realizado deberán de firmar y admitir que saben de estas políticas. El incumplimiento de estas normas será sancionado dependiendo del grado y norma a incumplir.
23. **Nuevos Trabajadores.** Todos los nuevos trabajadores se les informará que deben de leer un documento sobre las conductas y políticas que posee la empresa, para ellos serán llevados a una sala especial y serán supervisados por un personal de la empresa el cual, una vez terminado de leer, se les pedirá firmar un documento en donde reconoce que sabe de las políticas y conductas que debe de tener dentro y fuera de la empresa.
24. Planificación del Procedimiento de Actualización.

Para realizar un procedimiento de actualización se requiere de un plan, y cada plan se estructura según el proceso de actualización.

Se debe planificar la actualización de manera que se pueda saber que cambios a sufrido el sistema respecto a su versión anterior, tanto a nivel de comportamiento de la infraestructura, documentación existente, las características que han sido descartadas, la compatibilidad que se mantiene entre versiones y los requerimientos del entorno de producción.

Es importante que durante la planificación se realicen pruebas sobre el sistema, con el fin de identificar las aplicaciones e infraestructura actual, y posterior a la implementación realizar las mismas pruebas e identificar las salidas, si estas son correctas respecto a las actualizaciones.

Durante este proceso se deben considerar las siguientes tareas (IBM, s.f.):

1. Recopilación de la información necesaria, como las entradas requeridas y las salidas previstas de cada fase.
2. Evaluar las aplicaciones en el entorno de creación de informes y agrupar los informes similares
3. Instalar el nuevo software en un entorno de prueba y desplegar el contenido en el entorno de prueba
4. Probar las aplicaciones actualizadas para asegurarse de que los informes se ejecuten según lo esperado.

Por regla general, en el desarrollo de software y en el testing los procesos suelen ser iterativos, cuando se cuente con la certeza de que todas las funcionalidades son correctas, se deben migrar las actualizaciones o el nuevo sistema a producción

La creación de un plan de actualización contempla las siguientes actividades:

1. Revisión de los recursos, tales como la documentación.
2. Verificación de los entornos soportados para garantizar la compatibilidad entre actualizaciones.
3. Evaluación del sistema existente para determinar que desea mover a la nueva versión del producto.
4. Creación de un plan detallado para implementar la estrategia de actualización.

La utilización de la información adquirida a partir del sistema en desarrollo será utilizada para la creación de los sistemas de control de calidad y/o producción.

**FAQs:**

1. ¿Cuáles son los cambios respecto a la versión anterior?  
     
   Actualmente se implementan las mejores practicas en manejo de información, por lo que los cambios son principalmente a nivel organizativo, de gobierno y manejo de la información, por lo que los cambios incluyen tópicos como políticas de seguridad, asignación de roles a los usuarios, otorgándoles un puesto con ciertas atribuciones, formas de seguridad para la continuidad operacional y la seguridad en los procesos, una campaña de concientización sobre los efectos de las malas prácticas en el ámbito de responsabilidad con los datos e información, también contiene la estructura planificadora de las actualizaciones, y la forma de informar sobre todo lo anterior.
2. ¿Con quién contacto en caso de problemas?  
     
   En caso de presentar problemas con la nueva implementación se debe enviar un correo a upgrade@jetblack.cl, en caso de problemas de otra índole contactar a support@jetblack.cl.
3. ¿Cuánto tiempo demora que mi petición sea atendida?  
     
   El tiempo de respuesta normal es de un día hábil, es probable que tome mas tiempo por la naturaleza de la incidencia o si esta misma se repite en toda la organización, en tal caso se procederá a informar a todos mediante un correo general y los procedimientos para palear la situación.
4. ¿Cuáles son los medios de comunicaciones oficiales de la organización?  
     
   La empresa cuenta con el dominio jetblack.cl, por lo que todos los mensajes que contengan este remitente en su identificación corresponden a parte de la organización autorizada a emitir mensajes a internos o externos, esto esta limitado por los roles que cada cual ejerce.
5. ¿Cómo puedo realizar Backup de mis datos?  
     
   Para el rescate de los datos puede contactar con soporte, para tener una atención mas personalizada al respecto, de otra forma puede utilizar los repositorios oficiales de jetblack que contienen los archivos y código fuente de los desarrollos llevados hasta la fecha.

**Documentación**

Los recursos de documentación se pueden encontrar en los repositorios correspondientes por proyecto, para ubicar la documentación de los cambios en la estructura organizacional de la empresa se debe visitar los apartados N°1, 2, 3, 4 de este documento.  
  
 **Entornos soportados**

El anterior proyecto esta soportado en un entorno COBIT 5, para la integración de gobierno corporativo y los recursos de infraestructura informática, por lo que se trata de un marco de acción bastante flexible para la integración de nuevas características a la empresa.  
  
 **Auditoria**

1. Planificación de las fechas a realizar la auditoria.
2. Auditoria de procesos en conjunto con los dueños de estos mismos.
3. Realización de la auditoria.
4. Informar sobre la auditoria a los sectores que presenten problemas.
5. Seguimiento de las mejoras planteadas.

**Estudios**

Se realizan los estudios pertinentes con respecto a la previa auditoria recibida, con el propósito de identificar los cursos de acción adecuados en el marco de solventar los problemas detectados durante la fase anterior, la ventaja que un modelo así proporciona es la mirada de una entidad externa sobre la valides de los procesos construidos por la empresa a lo largo de sus años de servicio, y desde un punto imparcial poder mejorarlos y de esta forma solventar los problemas detectados.

**Recursos disponibles**

Podemos detectar los recursos de los que dispone la empresa desde un punto de vista externo, gracias a las actividades comerciales que ejercen, y de esta forma inferir con que recursos disponen a nivel tecnológico, que es lo que nos convoca.

Los activos que una empresa posee se clasifican dependiendo de su liquidez, es decir, la facilidad con la que ese activo puede convertirse en dinero. Por ello se dividen en:

1. **Activos tangibles**
   * Casa matriz de operaciones Región Metropolitana.
   * 4 sucursales: La Serena, Coquimbo, Ovalle y Tongoy.
   * Documentos legales de la institución.
   * Registro diario de la normativa asociada a contratos y proyectos.
   * Sistema de contabilidad de centro.
   * Políticas contables para que las cuentas operen bajo bases eficientes y consistentes.
   * Definición y asignación de responsabilidades de funcionarios y empleados.
   * Catálogo de cuentas y guía contabilizadora.
2. **Activos intangibles**

* Presta de servicios jurídicos en:
  + Elaborar y revisar la documentación de carácter legal en la institución. **(oficios, resoluciones, convenios, contratos, etc.)**
  + Elaborar el registro diario de la normativa vinculada a Contratos y Proyectos, publicada en el Diario Oficial.
  + Asesorar a la Secretaría en asuntos legales en que tenga participación la institución.
  + Atender consultas de las áreas técnicas de las áreas tecnológicas, contables y de Edificación.
* Presta de servicios contables en:
  + Establecer y operar las medidas necesarias para garantizar que el sistema de contabilidad del Centro este diseñado para que su operación facilite la fiscalización de los activos, pasivos, ingresos, costos y gastos de la organización.
  + Realizar las acciones necesarias para garantizar que el sistema contable del organismo, así como las modificaciones que se generen por motivos de su actualización, cuenten con las autorizaciones legales para su funcionamiento y operación.
  + Llevar a cabo la contabilidad del Centro en los términos que establece la Ley de Presupuesto, Contabilidad y Gasto Público.
  + Emitir por escrito las principales políticas contables necesarias para asegurar que las cuentas se operen bajo bases eficientes y consistentes, así como para la clara definición y asignación de responsabilidades de funcionarios y empleados.
  + Emitir por escrito las principales políticas contables necesarias para asegurar que las cuentas se operen bajo bases eficientes y consistentes, así como para la clara definición y asignación de responsabilidades de funcionarios y empleados.
  + Registrar y controlar los recursos financieros provenientes del calendario financiero presupuestal, los que otorgan las instituciones para el desarrollo de proyectos de investigación, así como los ingresos de donativos provenientes de dependencias y entidades del sector público, privado o social, identificando dentro de la contabilidad, los recursos aportados por instituciones públicas y privadas, destinados a proyectos específicos.
  + Elaborar, analizar y consolidar los Estados Financieros del Centro y de las Unidades Foráneas.
* Presta de servicios tecnológicos en:
  + Desarrollo de Sistemas. Analizar, diseñar y desarrollar los sistemas informáticos y supervisar aquellos que son de responsabilidad de contrapartes externas.
  + Desarrollo de Sistemas. Analizar, diseñar y desarrollar los sistemas informáticos y supervisar aquellos que son de responsabilidad de contrapartes externas.
  + Entrega de servicios electrónicos **(PC, correos, internet, software, etc.)**. Administrar y asegurar la disponibilidad de las redes, comunicación, servidores y estaciones de trabajo.
  + Investigaciones e innovación de tecnología. Buscar y proponer nuevas herramientas o estándares tecnológicos que aporten al desarrollo institucional en términos de mejoras en los procesos del Servicio.
  + Servicios Importantes con los que cuenta la Organización y son responsabilidad del Área. Servidor Documental de Jurídico, Servidor de Sistema SAP, Servidor de Dominio, Servidor de Intranet y Servidor de Correo.

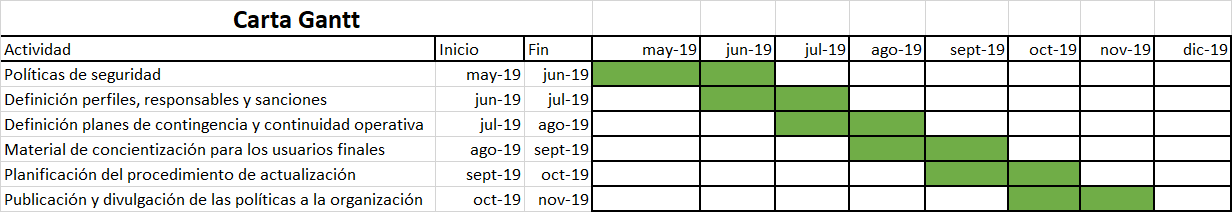
***Esta área cuenta con subdivisiones de especialidades que están conformadas por distintos expertos en el área, su enumeración y función a continuación:***

1. Unidad de desarrollo:
   * Administra las redes y servicios de telecomunicaciones.
   * Mantención de la seguridad en la red.
   * Mantención y administración a los servidores de documentos jurídicos, servidor de sistema SAP, servidor de dominio, servidor de intranet y de correo.
   * Respaldo de información.
2. Unidad de soporte:
   * Mantenimiento correctivo sobre hardware y software.
   * Soporte a todas las sucursales tanto en terreno como mediante telecomunicaciones.
   * Recepción de hardware con fallas.
   * Instalación de software en casos necesarios.

1. **Activos humanos**

* 300 funcionarios con 100 flotantes por año.
* Trabajadores de planta.
* Trabajadores a contrata.
* Trabajadores Honorarios.
  + Departamento de jurídico.
  + Departamento de contabilidad y finanzas.
  + Departamento de TI.
    - Unidad de desarrollo.
    - Unidad de sistemas.
    - Unidad de soporte.

**Hitos**



**Pruebas**

Para las pruebas se debe generar una estructura de feature test, los que se configuran con las salidas y entradas esperadas, y se comparan con los reales, y mediante este método se logra saber si el método en cuestión funciona como se espera, y en caso contrario, poder identificarlo y repararlo oportunamente.

**Recursos**

A nivel de recursos, es importante alinear la estructura de la empresa a los objetivos organizacionales, todo esto a través de los recursos disponibles, los cuales, mediante trabajos y transformaciones de productos o servicios, los transforman en valor, lo que actualmente se busca mejorar.

1. Publicación y divulgación de las Políticas a la Organización.

Para este propósito, el equipo de informática esta a cargo de la red de distribución de la información que distribuye la información a todo usuario que le corresponda por permisos.

Los métodos seleccionados serán principalmente redes sociales, tales como WhatsApp, Facebook y Twitter, los que en la actualidad son las redes sociales mas influyentes.

Esta campaña también contempla la concientización de los usuarios hacia las buenas practicas mediante afiches y eventos que se realizaran a lo largo del tiempo de puesta en marcha de las nuevas políticas.

Los usuarios deben estar involucrados en este proceso de manera activa, debido a que son los principales afectados en los cambios organizacionales, por lo que lograr una integración suave es importante para los niveles de estrés y adaptación de estos mismos.

La idea de presentar afiches es introducir de forma inconsciente los nuevos conceptos que deben ser digeridos al momento de la puesta en marcha, para que todo funcione según la nueva estructura de entradas procesos y salidas.

Es importante actuar en el marco de todos los sentidos de los usuarios, a nivel visual, sonoro, y otros que sean apropiados.

1. Conclusión

Al concluir el análisis podemos concluir que la transformación que sufre una empresa al momento de implementar las mejores practicas en el resguardo de su información requieren de un extenso trabajo sobre el reconocimiento de los procesos actuales en la empresa su actual infraestructura TI.

Basado en esto, tomar las medidas necesarias para el resguardo de la información, la igual que las personas, cada empresa tiene sus propiedades a nivel logístico y en la articulación de los procesos de negocio, lo que lo transforma en un ente único, comúnmente llamado agente de mercado, por lo que extrapolar las recomendaciones de seguridad requiere de adaptar tales prácticas a la realidad.

Las ventajas de esta implementación incluyen el aumento en la competitividad de la empresa por tres motivos:

**1-**  Estructura sus procesos de negocio y personas de la manera óptima para conseguir los objetivos de la organización.

**2-**  Resguarda la operación del negocio para brindar seguridad y confiabilidad a los clientes.

**3-**  Estos procesos son fácilmente auditables, lo que facilita mejorar el nivel CMM o ISO en la organización, lo que a su vez permite acceder a licitaciones antes limitadas por la estructura organizacional.

Mejorar la estructura en la empresa también tiene un rol motivador en los trabajadores, esto motivado por la claridad en los objetivos que tiene cada uno y como esto se conecta con sus compañeros de trabajo, dando un sentido tangible a el trabajo realizado y concientizando de la importancia de este.

Es importante para una organización mantener a sus trabajadores motivados por varios motivos, dentro de los cuales encontramos:

1. **Compromiso y rendimiento:** Para los trabajadores es importante identificarse con su empresa y sentirse orgullosos de pertenecer a la organización, lo que les brinda de manera intangible un aumento en la calidad de vida de estos mismos, al sentirse realizados a nivel personal.
2. **Mejoras en la imagen empresarial:** Es importante para los potenciales clientes y las posibles licitaciones a futuro tener una imagen corporativa responsable con el medio y sus trabajadores, y que al mismo tiempo apliquen las mejores practicas en distintas estructuras de trabajo, teniendo especial relevancia la seguridad.
3. **Mayor competitividad:** Esta comprobado que trabajadores motivados rinden con mayor calidad, esto basado en una relación de conformidad entre las partes empleador y empleado.

1. Referencias bibliográficas

Cesar Farro, C. F. (2018). *¿ Como concientizar a los colaboradores de una empresa sobre los riesgos de seguridad de la informacion?* Obtenido de ¿ Como concientizar a los colaboradores de una empresa sobre los riesgos de seguridad de la informacion?: https://medium.com/@cesarfarro/como-concientizar-sobre-los-riesgos-de-información-en-mi-empresa-7a0594e80abc

IBM. (s.f.). *ibm.com*. Obtenido de ibm.com: https://www.ibm.com/support/knowledgecenter/es/SSEP7J\_11.0.0/com.ibm.swg.ba.cognos.inst\_cr\_winux.doc/c\_upgrade\_upgradeprocess.html

SEK, P. R. (2009). *Universidad Internacional SEK Chile*. Obtenido de Universidad Internacional SEK Chile: https://www.usek.cl/media/1378/politicas\_uisek2009.pdf