**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](#_Toc8118667)

[II. Políticas de Seguridad. 4](#_Toc8118668)

[III. Definición perfiles, responsables y sanciones. 7](#_Toc8118669)

[IV. Definición Planes de Contingencia y Continuidad Operativa. 8](#_Toc8118670)

[V. Material de Concientización para los Usuarios Finales. 11](#_Toc8118671)

[VI. Planificación del Procedimiento de Actualización. 14](#_Toc8118672)

[VII. Publicación y divulgación de las Políticas a la Organización. 14](#_Toc8118673)

[VIII. Referencias bibliográficas 15](#_Toc8118674)

1. Introducción.
2. 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. **Políticas del Área de Sistemas y Soporte.**
11. Todos los equipos deberán presentar las últimas actualizaciones de Windows, parches de seguridad y antivirus instalado.
12. Los equipos de toda la agencia deberán de estar conectados a un regulador de corriente, como medida de prevención de variaciones de electricidad.
13. 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.
14. 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.
15. Una vez al año se realizará una revisión en la red para detectar desperfectos y dar así mantenimiento a la agencia.
16. 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.
17. 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.
18. **Políticas del Usuarios Finales.**
19. Cada empleado tiene establecido un equipo de cómputo al cual debe ingresar con un usuario y contraseña.
20. 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.
21. 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.
22. 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.
23. **Políticas del Área de Gestión.**
24. Gestionar el desarrollo de los sistemas informáticos de la Subsecretaría, tanto para los desarrollos propios o externalizados.
25. Supervisar el desarrollo de sistemas por parte de proveedores de servicios.
26. Administrar los sistemas productivos de la Subsecretaría y mantener la operatividad de los sitios WEB Institucionales.
27. Detectar, diseñar e implementar mejoras en los sistemas de gestión interna.
28. Revisión permanente de nuevas tecnologías que permitan mejorar las soluciones ya existentes.
29. Definición perfiles, responsables y sanciones.
30. 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.
25. Publicación y divulgación de las Políticas a la Organización.

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

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