Plan 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 |