1. **PLANIFICACION**
   1. **INTRODUCCION**

En el mundo de los negocios, la tecnología del cómputo ha incrementado su campo de acción desde transacciones de contabilidad de tabulación histórica, hasta asimilaciones de tiempo real en el manejo de datos complejos analógicos y digitales, así como en la formulación y la ejecución de procesos en procedimientos de control y seguridad. Las computadoras han adquirido la capacidad de asimilar consistentemente los datos, variables, soluciones de desarrollo, y aplicarlos a la multitud de problemas de negociación. En general, la mayoría de los procesos para la toma de decisiones y los sistemas de control que han sido institucionalizados en sistemas computacionales.

Para la mayoría de las organizaciones la supuesta dependencia de los sistemas de cómputo durante un periodo de recuperación de desastres es un mito propiciado por los siguientes factores:

Ausencia en una conciencia centralizada y en la prioridad de los Programas de Educación para tener un análisis del impacto en los negocios.

Fallas en la exploración de las alternativas

Un proceso educativo y la exploración de alternativas viables con el personal adecuado es la clave para la efectividad de los planes de contingencia a un costo adecuado.

La responsabilidad de llevar a cabo esta planeación dentro de las áreas funcionales de una organización puede ser asumida por departamentos individuales, sin embargo la planeación de contingencia debe ser coordinada centralizadamente. De forma tal que las relaciones interdepartamentales, las dependencias de un sistema con otros, y la necesidad de reducir duplicación de tareas en algunos puntos de la planeación justifican la necesidad de coordinar los procesos durante la planeación de contingencias en la corporación-completa.

* 1. **OBJETIVO GENERAL**

Revisar y Evaluar los planes de contingencias, procedimientos que utilizan en caso de una contingencia, su utilización, eficiencia y seguridad, a fin de que por medio de la auditoria se logre un mejor plan de contingencia que servirá para una adecuada toma de decisiones.

* 1. **OBJETIVOS ESPECIFICOS**
* Evaluar el diseño y prueba de los planes de contingencia
* Determinar la veracidad de los planes de contingencia
* Evaluar los procedimientos para cada tipo de contingencia, y evaluar la eficiencia de los mismos.
* Verificar las disposiciones y reglamentos que coadyuven a los planes de contingencia.
  1. **ALCANCE**

Nuestro examen se efectuará de acuerdo al enfoque que normalmente se aplica en las auditorías que realizamos, utilizando los lineamientos y el control de calidad que incluye un adecuado planeamiento que nos permite familiarizarnos con los procedimientos usados, con el propósito de cumplir con las Normas de Auditoría Generalmente Aceptadas. El alcance de nuestro examen será determinado después de haber adquirido una adecuada comprensión del sistema de control interno, lo cual nos permitirá identificar los procedimientos de auditoría que debemos aplicar.

* 1. **PROGRAMA DE AUDITORIA**

|  |  |  |
| --- | --- | --- |
| **No.** | **Procedimientos de auditoria** | **Tiempo Estimado** |
| Fase I | Planificación  Visita Preliminar   * Solicitud de Manuales y Documentaciones. * Elaboración de los cuestionarios. * Recopilación de la información | 1 SEMANA |
| Fase II | Trabajo de Campo   * Evaluación de la información recolectada * Análisis de riesgo * Hallazgos Potenciales | 1 SEMANA |
| Fase III | Comunicación de Resultados   * Observación * Recomendación * Conclusión | 1. DIAS |

* 1. **DOCUMENTOS SOLICITADOS**
* Políticas, estándares, normas y procedimientos.
* Plan de contingencias.
* Planes de seguridad y continuidad
* Organigrama y manual de funciones.
* Registros
* Entrevistas
* Archivos
  1. **METODOLOGIA**

Para llevar a cabo la auditoria y con el objetivo de recopilar la mayor información posible, se utilizo cinco herramientas que se describen a continuación.

1. Visitas

Se llevó a cabo visitas de auditoria a los responsables de proceso en las áreas en las que se lleva a cabo el mismo; con el objetivo de verificar y validar los planes de contingencia que utilizan, mediante la revisión de evidencia en la operación del proceso.

1. Revisión de la documentación

Se llevó a cabo una revisión de los planes de contingencia a fin de verificar el nivel de documentación que tienen declarados y poder constatar si a la fecha ya están al 100% documentados los procesos.

1. Encuestas

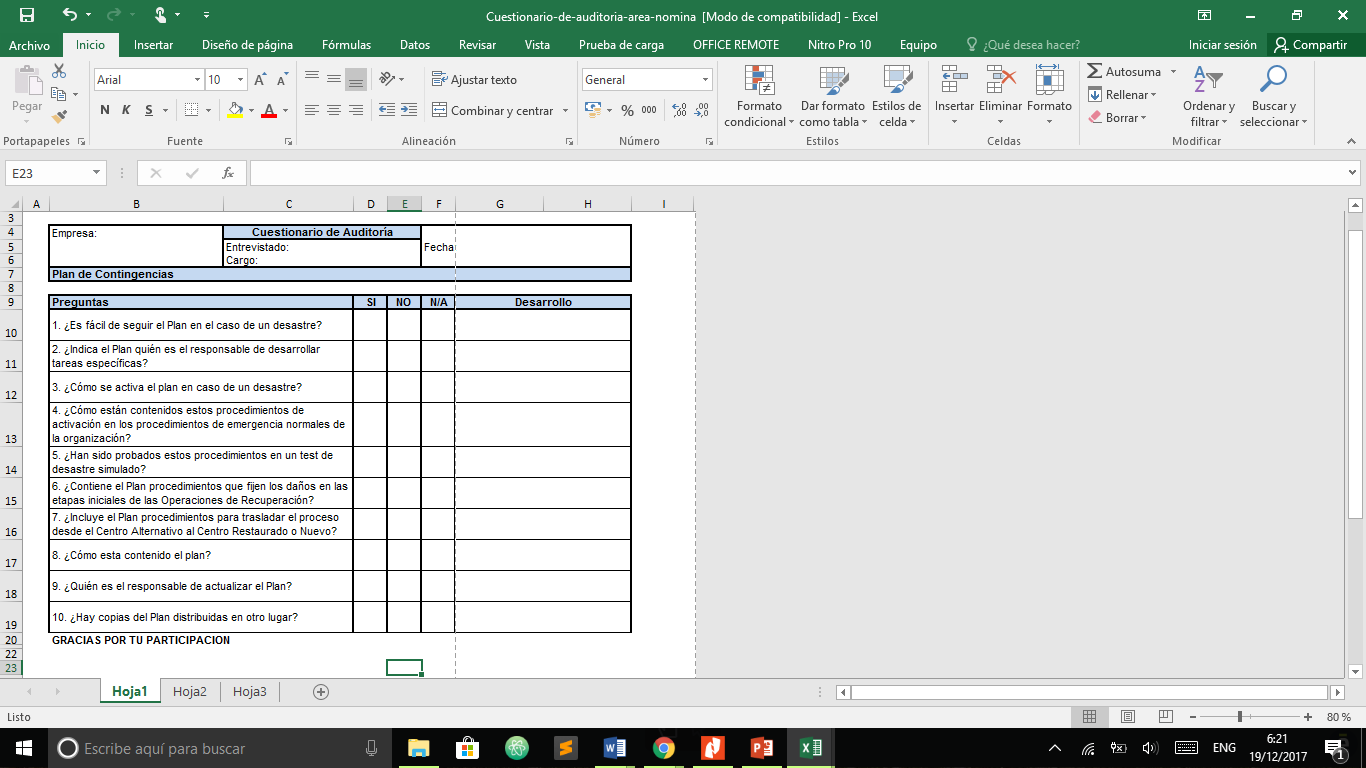
Se aplicó una encuesta de 10 preguntas al personal operativo presente al momento de la auditoria, con el objetivo de conocer la percepción del personal al uso de los planes de contingencia.

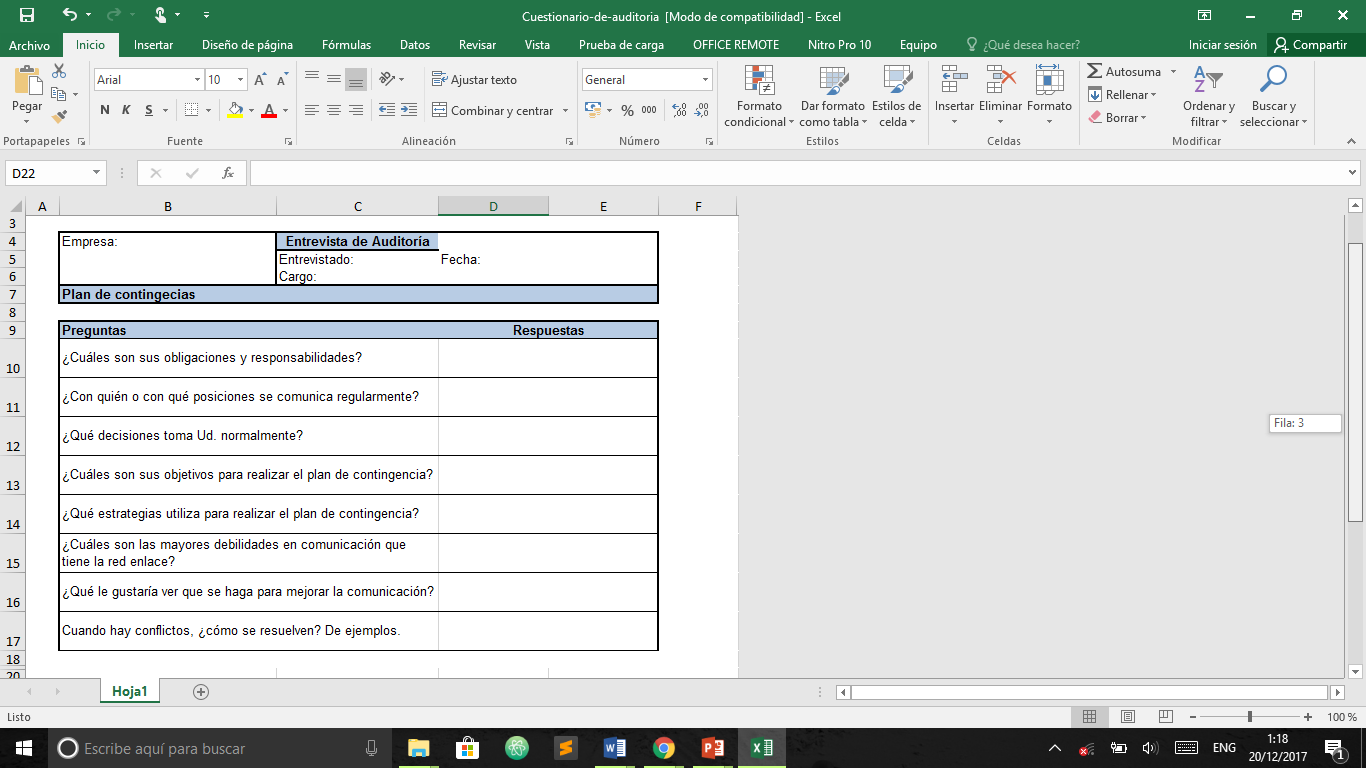
1. Entrevista

Responsables de la elaboración de planes de contingencia

Se realizó una entrevista al responsable del área a fin de conocer su percepción sobre la importancia de los planes de contingencias.

## **ENCUESTAS**



* 1. **ENTREVISTAS**

1. **TRABAJO DE CAMPO**

Establecido el plan y definidas las pruebas en el programa de auditoría, se inicia la fase de ejecución de la auditoría consistente en la obtención de evidencias suficientes y adecuadas para lograr una base de juicio razonable sobre la información contenida en la documentación de la empresa con el objetivo de expresar una opinión sobre las mismas, tal como establece la norma ISO 9001:2015 que especifica que hay que planificar, comprobar y revisar.

* 1. **OBJETIVO**

Verificar que lo mencionado en la entrevista con el represéntate de la institución, sea verídica y que existan referencias y evidencias de lo comentado en está, para con ello asegurar que se esté llevando eficientemente los planes de contingencias.

* 1. **HALLAZGOS POTENCIALES**
* Falta de plan de contingencia ante clonaciones de tarjetas de crédito en cajeros automáticos

Dando a conocer los resultados de nuestra auditoria a la red enlace en los cajeros automáticos consideramos que falta implementar algunos planes de Contingencias. Si bien hemos observado la existencia de normas, procedimientos y controles pero que no cubren todo en cuanto a seguridad de la información de las tarjetas de crédito y no son suficientes para este tipo de contingencias que se detallara a continuación:

1. La forma de robar de los delincuentes consiste en instalar dispositivos electrónicos falsos sobre los cajeros. El mecanismo funciona por medio de una banda magnética y un aparato de alta tecnología capaz de leer y copiar la información de las tarjetas.

Este tipo de robos, clonaciones es uno de los principales fraudes que sufren los usuarios que portan estas tarjetas.

La clonación de tarjetas de crédito es una modalidad de fraude que es la acción cometida intencionalmente para obtener ganancia de forma ilícita o ilegal.

Bajo el criterio de ubicación del agente o titular del acto fraudulento, el fraude puede ser interno o externo. El fraude será interno cuando es realizado por los mismos trabajadores de la institución bancaria, por ejemplo, sustracciones de dinero que se realicen en perjuicio del propio banco o de sus clientes. De igual modo, el fraude será externo cuando el sujeto activo es una persona ajena a la entidad, por ejemplo, robos, falsificaciones, penetración no autorizada en los sistemas informáticos. La clonación de tarjetas bancarias como acto fraudulento está ubicada dentro de los fraudes externos.

Existen una serie de formas, técnicas o tipologías que permiten utilizar una tarjeta de crédito como medio o instrumento para cometer fraudes. Están son algunas de las modalidades:

-      Falsificación de la banda magnética.

-      Tarjeta expedida con datos falsos.

-      Documento de identidad falso.

-      Retiros fraudulentos por cajero automático.

Las técnicas utilizadas por los delincuentes para clonar tarjetas de crédito son el phishing, trashing, sniffing, Boxing y skimming. Se dara a conocer la técnica usada para realizar este tipo de clonación.

El Skimming es la técnica de clonación más conocida y consiste en la utilización de un dispositivo denominado skimmer para copiar la información contenida en la banda magnética de la tarjeta. Mediante esta técnica se coloca en el cajero automático un pequeño aparato llamado skimmer que roba los datos de la banda magnética arrastrando la tarjeta. Luego el clonador retira el dispositivo y transfiere los datos de la tarjeta en un ordenador PC para posteriormente transferirla en una tarjeta en blanco.

1. **COMUNICACIÓN DE RESULTADOS**
   1. **INFORME DE AUDITORIA**

**Identificación del informe**

Auditoria plan de contingencias

**Identificación de la Entidad Auditada**

Red Enlace

* 1. **OBJETIVOS**
* Determinar las acciones preventivas, para reducir el grado de vulnerabilidad ante robos y exposición al riesgo.
* Implementar un plan de contingencias en cajeros automáticos que considere aspectos como robos de tarjetas de crédito para la red enlace en Bolivia.
* Proveer las recomendaciones de planes de contingencias para fortalecer los aspectos críticos que se presenten.

* 1. **OBSERVACIONES**
* Falta de plan de contingencia ante clonaciones de tarjetas de crédito en cajeros automáticos.
  1. **RECOMENDACIONES**

Bajo estas condiciones se recomienda a la red enlace aumentar la seguridad en los cajeros automáticos como los planes de contingencia que se dará a conocer a continuación:

1. Implementar un sistema que verifica la identidad de una persona a través de la mano, **basta con que el usuario ponga la palma en el lector** y el programa permitirá al individuo realizar su o peración si es el dueño de la tarjeta. El terminal le reconoce a través de una exploración geométrica, en función de la forma de la mano.
2. Implementar la detección a través de la huella dactilar, que es única para cada ciudadano. Este método favorece que la posibilidad de error o falsificación sea imposible.
3. Implementar la identificación del rostro a través de determinadas facciones de la persona. El usuario solo podrá obtener dinero del cajero si el semblante se ajusta al del propietario de la tarjeta.
4. Implementar la detección que se realiza a través del ojo, la biometría diferencia el iris de cada persona sin que quepa posibilidad de que haya dos iguales.

Para la seguridad de los cajeros se recomienda implementar:

* Instalar un sistema de control de accesos al cubículo de atención al público, considerando que puede ser mecánico o electrónico y además incluya un cierrapuertas.
  1. **CONCLUSION**

A través del estudio y del desarrollo de este trabajo, se ha logrado obtener conclusiones respecto a los planes de contingencia en los cajeros automáticos identificando las amenazas que perjudicaría al dueño de la tarjeta de crédito en caso de que no pueda utilizarla por extravió, robo o clonación de su tarjeta, también se realizó la recomendación para evitar este tipo de contingencias, así como un sistema de detección facial para reducir el grado de vulnerabilidad de los cajeros automáticos y dando a conocer a los encargados de la red enlace que no es “algo más” que hay que hacer, sino que es igual de importante o más que las otras partes del proyecto y es reconocida como una buena práctica profesional manejar la seguridad con mucha seriedad, desarrollando los planes de contingencia.

Por último, cabe señalar que es un delito el uso fraudulento de tarjeta de crédito, tal como la relación que le da origen, el uso de tarjeta de crédito, es un delito que está en constante movimiento y dinamismo. El número de tarjetas aumenta día a día, y los avances tecnológicos y del ingenio permiten nuevas formas de comisión del delito, y junto con ella viene la necesidad de generar nuevas interpretaciones que amparen los hechos, a fin de no dejar desprotegidos tanto a los usuarios de las tarjetas, como a cualquier posible víctima.