UNIVERSIDAD TECNOLÓGICA DEL CENTRO DE VERACRUZ

PROGRAMA EDUCATIVO DE:

TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

REPORTE PARA OBTENER TÍTULO DE:

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN EN COMPETENCIAS PROFESIONALES

PROYECTO DE ESTADÍA REALIZADO EN:

AUTOMOTRIZ GOMSA S.A. DE C.V.

UNIVERSIDAD TECNOLÓGICA DEL CENTRO DE VERACRUZ

PROGRAMA EDUCATIVO DE:

TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

NOMBRE DEL PROYECTO:

AUDITORÍA DE SEGURIDAD FÍSICA

P R E S E N T A:

JESÚS DANIEL ENRIQUEZ CONCEPCIÓN

ASESOR INDUSTRIAL:

ING. MIGUEL ÁNGEL GARCÍA RAMÍREZ

ASESOR ACADÉMICO:

MCC. LORENA ALCUDIA CHAGALA

Córdoba, Veracruz , miércoles, 13 de abril de 2016

RESUMEN

Se comprende por auditoría informática de seguridad que abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan, contemplando las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

Tomando como referencia el concepto anterior, el objetivo de este protocolo es llevar a cabo un análisis de la situación en la que se encuentra la empresa automotriz GOMSA ubicada en el boulevard Córdoba-Peñuela de la ciudad de Córdoba, Veracruz; de acuerdo al ámbito de la seguridad informática, se desarrollará una correcta auditoría, se definirá posibles amenazas y se evaluará la seguridad física de la empresa. Dicha auditoría pretende que mediante el uso de medidas de seguridad y de normas o estándares se evalúe la seguridad física de la empresa.

Para desarrollar está auditoría de seguridad física, nos apoyaremos de la norma internacional ISO 27002, que nos permitirá tener una disminución de siniestros, trabajar mejor en el mantenimiento de la seguridad y detección de incidentes, con el fin de tener planes de contingencias, contención ante accidentes y para llevarse un mejor control de todos los accesos lógicos y obtener beneficios óptimos en la empresa.

ABSTRACT

It understood by computer security audit covering the concepts of physical security and logical security. Physical security refers to the protection of hardware and data carriers, as well as buildings and facilities that house, watching the fire situations, sabotage, theft, natural disasters, etc.

Taking the above concept, the aim of this protocol is to conduct an analysis of the situation in which the automaker GOMSA located on Boulevard Cordoba-Peñuela city of Cordoba, Veracruz is located; according to the field of computer security, a proper audit will be developed will be defined threats and physical security of the company will be assessed. The audit intended that using safeguards and physical standards or safety evaluate standards of the company.

To develop this audit of physical security, we will rely on the international standard ISO 27002, which allow us to have a decrease in accidents, work better in the maintenance of security and incident detection, in order to have contingency plans, containment before accidents and to take better control of all logical access and optimum benefits in the company.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

INTRODUCCIÓN

Durante mucho tiempo se consideró que los procedimientos de auditoría y seguridad era responsabilidad de la persona que elabora los sistemas, sin considerar que es responsabilidad del área de informática en cuanto a la utilización que se le da a la información, la forma de accesarla y del departamento de auditoría interna en cuanto a la supervisión y diseño de los controles necesarios.

La seguridad del área de informática tiene como objetivos:

- ✓ Proteger la integridad, exactitud y confidencialidad de la información.
- ✓ Proteger los activos ante desastres provocados por la mano del hombre y de actos hostiles.
- ✓ Proteger la organización contra situaciones externas como desastres naturales y sabotajes.
- ✓ Etc.

Las medidas de seguridad física servirán para proteger nuestros equipos e información frente a usos inadecuados, fallos de instalación eléctrica, accidentes, robos, atentados, desastres naturales, y cualesquiera otros agentes que atenten directamente contra su integridad física. La importancia de este tópico en la empresa GOMSA permitió llevar a cabo este protocolo de investigación, en el cual se presenta los siguientes capítulos.

CAP I: Antecedentes: Se presenta de forma breve el problema que tiene la empresa automotriz GOMSA, donde se llevará acabo la auditoría de seguridad física. Se da a conocer el objetivo que tendrá la aplicación de dicha auditoría y cuáles serán las metas específicas que deberán cumplirse, para lograr el objetivo principal. Al igual en este capítulo se aborda el alcance que debe cubrir la auditoría de acuerdo a la investigación realizada, así mismo las posibles limitaciones que tendrá en su aplicación y se presenta de forma concreta y precisa la justificación de la solución al problema que se origina en la empresa.

CAP II. Marco Teórico: Se hace mención en este apartado, sobre las herramientas a utilizar, así como detalles de las mismas, considerando la justificación de su uso.

CAP III. Metodología: Se realiza un análisis y se lleva acabo el desarrollo de esta auditoría de seguridad física haciendo referencia de la metodología que se expone en este documento con la finalidad de llevar a cabo su aplicación.

CAP IV. Procedimientos: Se explica y se da a conocer los formatos que se aplicarán en el desarrollo de la auditoría de seguridad física, así mismo formatos correspondientes y aplicados según la norma ISO 27002, haciendo uso de las fases de la metodología COBIT.

CAP V. Evaluación de resultados: Con respecto a la metodología COBIT se realizan las posibles evaluaciones para obtener resultados y generar posibles recomendaciones de mejora de seguridad física y de procesos

CAP VI. Conclusiones: Conclusión con respecto al proyecto realizado referente a la seguridad física.

CAP VII. Referencias bibliográficas. Se presentan una serie de citas bibliográficas de las cuales fueron tomadas como referencias para realizar aportaciones a este protocolo.

CAP VIII. Anexos. Anexos.

La aportación central de este protocolo es difundir los beneficios que puede ofrecer el desarrollo de una auditoría de seguridad física, proponiendo una metodología con el objetivo de obtener una mejor eficiencia a la hora de llevar a cabo dicha auditoría.

CÁPITULO 1

1.1 Antecedentes

1.1.1 Antecedentes de la empresa

Grupo GM, nace en el año 2008 fruto de la escisión de grupo GOMSA, empresa con más de 150 años de existencia y tres generaciones de dirigirla. A pesar de la corta historia como grupo GM, las empresas que lo conforman tienen una importante trayectoria y tradición de más de 35 años en el estado de Veracruz y Oaxaca.

En el ramo automotriz contamos con la distribución de las marcas chevrolet, buick-gmc y cadillac en las ciudades de Veracruz, Xalapa, Orizaba, Córdoba, Tierra Blanca, Acayucan, Martínez de la Torre – Veracruz, Teziutlán - Puebla y Tuxtepec - Oaxaca.

Al mismo tiempo se conserva la participación dentro de grupo GOMSA, dedicado al ramo de comercio exterior y transporte logístico. En el ramo de logística internacional se cuenta con agencias aduanales, oficinas de comercialización, bodegas y líneas de transporte.

1.1.2 Misión

Ofrecer productos y servicios que generen entusiasmo en nuestros clientes.

1.1.3 Visión

Ser reconocidos por General Motors como los mejores distribuidores de México con la distinción de “distribuidores oro”.

1.1.4 Valores

- ✓ ***servicio***._ porque es nuestra razón de ser.
- ✓ ***profesionalismo***._ porque es la base de nuestro liderazgo.
- ✓ ***calidad***._ porque es el resultado de nuestra gestión.
- ✓ ***tradición***._ porque es el mejor exponente de futuro.
- ✓ ***creatividad***._ porque es el germen de los grandes éxitos.
- ✓ i***nnovación***._ porque es una exigencia de la modernidad.
- ✓ ***compromiso***._ porque es nuestra contribución a la sociedad.
- ✓ ***dinamismo***._ porque es la clave de nuestra eficiencia.
- ✓ ***capacidad de respuesta***._ porque es el soporte de atención al cliente.
- ✓ ***creación de riqueza***._ porque es la garantía de nuestro crecimiento.
- ✓ ***organismo vivo***._ porque es indispensable para la evolución.
- ✓ ***orientados al mercado***._ porque es el fundamento de nuestra oferta comercial.

1.1.4.1 Compromisos

Satisfacción Total del Cliente.

En grupo GM, siempre con una sonrisa y actitud de servicio, buscamos superar las expectativas de nuestros clientes, a través del conocimiento de nuestros productos y servicios, que nos permitan agilizar la toma de decisiones, asegurando su preferencia y haciendo del servicio al cliente una ventaja competitiva en nuestro negocio.

Un Gran Lugar para Trabajar.

En grupo GM, estamos comprometidos con la selección, capacitación, desarrollo y crecimiento profesional de nuestra gente, que nos permita ser un referente en talento humano.

Medio Ambiente

Todos en grupo GM, conscientes de nuestro entorno, fomentamos una participación activa, apoyando programas de desarrollo sustentable, empleando eficientemente nuestros recursos, reduciendo los residuos generados y mejorando nuestro impacto al medio ambiente.

1.2 Planteamiento del problema

La empresa GOMSA automotriz, S.A. de C.V. ubicada en la calle 43 s/n esq. Blvd. Córdoba-Peñuela col. zona industrial, empresa dedicada a la comercialización de vehículos, refacciones y mantenimiento automotriz, desea tener un buen uso de los equipos de cómputo dentro de las áreas en las que se desempeña el trabajo. Actualmente dicha empresa necesita estar a la vanguardia, sobre todo de un buen funcionamiento del equipo con los que cuenta, además de tener una seguridad física que permita tener protegido los sistemas de información, así mismo detectar las posibles vulnerabilidades de los que no se tiene conocimiento, haciendo uso de la norma ISO 27002 con el fin de buscar reducir los siniestros, trabajar adecuadamente para lograr una seguridad optima y detectar posibles amenazas y mantener la seguridad física correcta.

1.3 Objetivo General

Realizar una auditoría de seguridad física en la empresa automotriz GOMSA S.A de C.V, con el fin de identificar posibles vulnerabilidades existentes relacionadas a controles de seguridad, haciendo uso de la norma ISO 27002, con el propósito de implementar un modelo de seguridad y verificando la integridad de los activos.

1.4 Objetivos específicos

- Elaborar un plan estratégico de auditoría que especifique las actividades que se implementarán durante su desarrollo.

- Evaluar y verificar los accesos a los sistemas de información para determinar si son adecuados y eficientes.

- Verificar el uso adecuado de la información proporcionada por la empresa (manuales).

- Realizar una auditoría factible para poder combatir los problemas que se presenten con respecto a la seguridad física de la empresa.

- Evaluar los componentes físicos de la información de la empresa.

- Elaborar un informe del diagnóstico de la infraestructura auditada.

- Generar propuestas de solución y mejora que atiendan a las anomalías documentados en el diagnóstico de la auditoría.

1.5 Justificación

El presente protocolo tiene como objetivo principal de ayudar en el cumplimiento de las funciones y responsabilidades, de la seguridad física de la empresa automotriz GOMSA, donde se ha identificado que es necesario llevar a cabo una auditoría para aportar recomendaciones de mejoras a la situación actual de la empresa, y con ello determinar un plan de acciones que puedan atender los problemas relacionados al tráfico de información, así como el control asignado a cada empleado.

Uno de los impactos más importantes que este proyecto aportará a la organización, es la identificación e áreas de oportunidad que al ser atendidas puedan disminuir las posibles contingencias y amenazas.

CAPÍTULO 2

2.1 Marco Teórico

COBIT

El COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores TIC, usuarios y por supuesto, los auditores involucrados en el proceso. Modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad TIC y que abarca controles específicos de TIC desde una perspectiva de negocios.

Las siglas COBIT significan objetivos de control para tecnología de información y tecnologías relacionadas (control objectives for Information systems and related technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (information systems audit and control association).

COBIT, lanzado en 1996, es una herramienta de gobierno de TIC que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

MISIÓN DEL COBIT

Buscar, desarrollar, publicar y promover un autoritario y actualizado conjunto internacional de objetivos de control de tecnologías de la información, generalmente aceptadas, para el uso diario por parte de gestores de negocio y auditores.

BENEFICIOS COBIT

- Mejor alineación basada en una focalización sobre el negocio.
- Visión comprensible de TIC para su administración.
- Clara definición de propiedad y responsabilidades.
- Aceptabilidad general con terceros y entes reguladores.
- Entendimiento compartido entre todos los interesados basados en un lenguaje común.
- Cumplimiento global de los requerimientos de TIC planteados en el marco de control interno de negocio coso.

ESTRUCTURA

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

La adecuada implementación del modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

DOMINIOS COBIT

El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales, a saber:

Planificación Y Organización: Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes

perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Adquisión E Implantación: Para llevar a cabo la estrategia de TIC, las soluciones de TIC deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Soporte Y Servicios: En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Monitoreo y Evaluación: Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

USUARIOS

La Gerencia: Para apoyar sus decisiones de inversión en TIC y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.

Los Usuarios Finales: Quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

Los Auditores: Para soportar sus opiniones sobre los controles de los proyectos de TIC, su impacto en la organización y determinar el control mínimo requerido.

Los Responsables de TIC: Para identificar los controles que requieren en sus áreas.

También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TIC en las empresas.

CARACTERÍSTICAS

- Orientado al negocio.
- Alineado con estándares y regulaciones "de facto".
- Basado en una revisión crítica y analítica de las tareas y actividades TIC.

(COBIT, 2007)

¿Qué es una auditoria?

La auditoría es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, que puede ser una persona, organización, sistema, proceso, proyecto o producto.

(contables, 2014)

¿Qué es un auditor?

Evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoria.

(Roldán, 2013)

¿Qué es Seguridad Física?

La seguridad física hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático, para proteger el hardware de amenazas físicas. La seguridad física se complementa con la seguridad lógica.

- Desastres naturales, incendios accidentales, humedad e inundaciones.
- Amenazas ocasionadas involuntariamente por personas.
- Acciones hostiles deliberadas como robo, fraude o sabotaje.

Son ejemplos de mecanismos o acciones de seguridad física:

- Cerrar con llave el centro de cómputos.
- Tener extintores por eventuales incendios.
- Instalación de cámaras de seguridad.
- Guardia humana.
- Control permanente del sistema eléctrico, de ventilación, etc.

(futuro, 2002)

Método

Palabra que proviene del término griego methodos (camino o vía) y se refiere al medio utilizado para llegar a un fin. Su significado original señala el camino que conduce a un lugar.

Las investigaciones científicas se rigen por el llamado método griego, basado en la observación y la experimentación, la recopilación de datos, la comprobación de las hipótesis de partida.

(Investigación, 2004)

Planeación

La planeación, también conocida como planificación o planeamiento, consiste en el proceso a través de cual se analiza la situación actual (dónde estamos), se establecen objetivos (dónde queremos llegar), y se definen las estrategias y cursos de acción (cómo vamos a llegar) necesarios para alcanzar dichos objetivos.

(Carvajal, 2011)

Plan

Programa detallado de la realización de una cosa y conjunto de medios para llevarla a cabo. Programa detallado de la realización de una cosa y conjunto de medios para llevarla a cabo.

(Copyright © 2003-2016 Farlex, 2011)

Programa

Proyecto o planificación ordenada de las distintas partes o actividades que componen el plan de trabajo y que se va a realizar: programa de actividades.

(Copyright © 2003-2016 Farlex, Programa, 2011)

Entrevista

La entrevista es una técnica para recolectar información para el desarrollo de la propuesta ya que mediante ella se llevan a cabo las reuniones de trabajo necesarias para conocer los objetivos del proyecto, sus requisitos, las opciones de diseño y los acuerdos con el cliente.

(de, 2001)

Cuestionario

El diseño de un cuestionario debe de tener una adecuada preparación, elaboración, pre evaluación y evaluación.

(Geografía, 2010)

Metodología

Una metodología es la ciencia que estudia un método, también se refiere a la serie de métodos y técnicas de rigor científico que se aplican sistemáticamente durante un proceso de investigación para alcanzar un resultado teóricamente valido.

La metodología de la investigación es una disciplina de conocimiento encargada de elaborar, definir y sistematizar el conjunto de técnicas, métodos y procedimientos que se deben seguir durante el desarrollo de un proceso de investigación para la producción de conocimiento.

(CONTACADEMICA, 2015)

Norma ISO 27002

Esta norma nos habla de seguridad física y ambiental con esta norma se implementara en buscar en reducir los siniestros, trabajar adecuadamente al tener seguridad y descartar las falsas hipótesis si se producen problemas.

(© Ministerio de Educación, 2010)

CAPÍTULO 3

3.1 Metodología

La implementación de COBIT es porque la metodología se centra en encontrar y eliminar las causas que producen defectos, mejora los procesos, productos y soluciona problemas, COBIT guía a las empresas hacia el objetivo de cometer el menor número de errores en las actividades que desarrollen, también aporta nuevos métodos específicos para volver a crear procesos de modo que los errores no vuelvan a producirse. la metodología consta de 4 fases *planificación y organización, adquisición e implantación*:, *soporte y servicios* y por ultimo *monitoreo y evaluación,* cada una de ellas lleva una estructura la cual hace que la metodología sea fácil de entender, esta será acompañada por la norma ISO 27002 la cual nos habla de seguridad física y ambiental con esta norma que se implementará se busca disminuir los siniestros, tener medios para atacar una contingencia, trabajar mejor teniendo seguridad y descartar falsas hipótesis si se producen siniestros.

COBIT

El COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores TIC, usuarios y por supuesto, los auditores involucrados en el proceso. Modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad TIC y que abarca controles específicos de TIC desde una perspectiva de negocios.

Las siglas COBIT significan objetivos de control para tecnología de información y tecnologías relacionadas (control objectives for information systems and related technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (information systems audit and control association).

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales y las redes. Está basado en la filosofía de que los recursos TIC necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

Planificación Y Organización: Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Adquisición E Implantación: Para llevar a cabo la estrategia de TIC, las soluciones de TIC deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Soporte Y Servicios: En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Monitoreo y Evaluación: Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

(COBIT, 2007)

CAPÍTULO 4

4.1 Procedimiento

Cabe mencionar que el concepto de procedimiento es un método de ejecutar una serie de pasos definidos que permite realizar un trabajo de forma correcta.

Durante el desarrollo de la auditoria de seguridad física se llevará a cabo la realización de formatos específicos para el levantamiento de información necesaria, con el fin saber cuáles son las condiciones actuales de la empresa y las mejorías que tendrá durante la aplicación de dicha auditoría con respecto a la seguridad física.

Dichos formatos son basados en la norma ISO 27002, ya que es una norma muy apegada de las auditorias de seguridad física.

Las medidas que se deben tener en cuenta antes de llevar a cabo la auditoria, es obtener y mantener un nivel adecuado de seguridad física sobre los activos.

Durante la aplicación de la auditoria se debe ejecutar un plan de contingencia, donde se debe conocer la información y tener presente que la prevención es uno de los recursos más viables y factibles para evitar que los riesgos provoquen daños severos, por lo tanto el plan de contingencia es necesario e indispensable que garantice el correcto restablecimiento del correcto funcionamiento de los servicios en el menor tiempo posible, ante cualquier eventualidad.

El plan de contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo tanto cabe destacar que dentro del plan de contingencia se incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo de forma rápida, con el menor costo y menor pérdidas posibles.

Es muy importante saber que cada entidad puede generar un plan de contingencia de acuerdo a sus necesidades y a la capacidad de recuperación que tengan, de igual manera depende mucho del presupuesto que se destine para ello, Dentro del plan de contingencia se comprenden 3 planes:

1) Plan de respaldo: Contempla medidas preventivas antes de que se materialice una amenaza, su finalidad es evitar dicha materialización.
2) Plan de emergencia: Contempla las medidas necesarias durante la materialización de una amenaza o inmediatamente después, su finalidad es contrarrestar los efectos adversos de la misma.
3) Plan de recuperación: Contempla las medidas necesarias después de materializada y controlada la amenaza, su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

Dentro del plan de contingencias deben estar contenida las siguientes contramedidas:

- *Medidas técnicas:*
    - Extintores contra incendios.
    - Detectores de humo.
    - Salidas de emergencia.
    - Equipos informáticos de respaldo.
- *Medidas organizativas:*
    - Seguro de incendios.
    - Precontrato de alquiler de equipos informáticos y ubicación alternativa.
    - Procedimiento de copia de respaldo.
    - Procedimiento de actuación en caso de incendio.
    - Contratación de un servicio de auditoría de riesgos laborales.
- *Medidas humanas:*
    - Formación para actuar en caso de incendio.
    - Designación de un responsable de sala.
    - Asignación de roles y responsabilidades para la copia de respaldo.

Los subplanes contendrían las siguientes previsiones:

Plan de respaldo: trata de cómo se llevan a cabo las acciones críticas entre la pérdida de un servicio o recurso, y su recuperación o restablecimiento. Todos los nuevos diseños de sistemas, proyectos o ambientes, tendrán sus propios planes de respaldo.

Respaldo de datos Vitales

Identificar las áreas para realizar respaldos:

a) Sistemas en Red.

b) Sistemas no conectados a Red.

c) Sitio WEB.

- El Plan de Respaldo debe contener:
  - Revisión de extintores.
  - Simulacros de incendio.
  - Realización de copias de respaldo.
  - Custodia de las copias de respaldo de información importante
- *Plan de emergencia*:
  - Activación del precontrato de alquiler de equipos informáticos.
  - Restauración de las copias de respaldo.
  - Reanudación de la actividad.

Plan de recuperación: la responsabilidad sobre el plan de recuperación es de la administración, la cual debe considerar la combinación de todo su personal, equipos, datos, sistemas, comunicaciones y suministros.

- El Plan de Recuperación debe contener
  - Evaluación de daños.
  - Traslado de datos desde la ubicación de emergencia a la habitual.
  - Reanudación de la actividad.

El plan de contingencia generará como resultado que recursos materiales son necesarios, como se debe cumplir, responsabilidades concretas y asignación de roles de cómo se debe llevar a cabo y por última fase se consideran las acciones a seguir.

A continuación, se muestra el cronograma de las actividades que se realizarán durante el desarrollo de la auditoría de seguridad física dentro de la empresa automotriz GOMSA S.A. de C.V. de la ciudad de Córdoba, Veracruz.

Tabla 1.1 1

TABLA DE INDENTIFICACIÓN DE RIESGOS		
Evidencia	Riesgo	Alternativa de solución
 *Ilustración 1.1 1*	En la foto, se muestra que el switch esta colocado cerca de la puerta, de salida de emergencia, así mismo se logra observar que no existe un cuarto donde se logre alojar el mismo. Se tiene el riesgo de sufrir daños severos, directamento al switch, esto es fisicamente.	Si es posible asignar un cuarto especial y exclusivo para el alojamiento del switch para evitar daños fisicos y en caso de algun desastre natural pueda recuperarse de forma rápida.
 ***Ilustración 2.1 1***  ***Ilustración 2.1 2***	En las fotos se logran apreciar el desamble de una computadora de escritorio, al mismo tiempo se le da mantenimiento, debido a los residuos de polvo y otros desechos dentro del equipo. Los riesgos más frecuentes que se originan por no dar mantenimiento a los equipos son, de que se puede dañar el equipo físicamente y al mismo tiempo puede producir fallos en el sistema, provocando perdida de datos e información valiosa. La acumulación de polvo daña al equipo severamente, tanto físico como lógicamente.	Es recomendable realizar un mantenimiento preventivo una sola vez por mes para evitar que los equipos sufran de lentitud a la hora de procesar, así mismo la durabilidad de los equipos de cómputo sean mayor a la que se tenía prevista

 *Ilustración 2.1 3*  *Ilustración 2.1 4*	Por lo que se recomienda que se realice o se lleve a cabo, un mantenimiento preventivo.	
 *Ilustración 3.1 1*	El riesgo que puede surgir de no usar canaletas para los cables de red son, estropear el cable, tropiezos del personal al pasar por encima del cable y daños fisicos del cable. Las canaletas son conductos o tubos en cuyo interior se guardan los cables, cuando estos no quedan empotrados en la pared. Cumplen así una doble función, ya que, por un lado, permiten organizar los cables a través de un sistema que se	El uso de canaletas evitara que sufra daños fisicos el cable y pueda ser mas durable, asi mismo evitar que el personal sufra caidas o cualquier otro tipo de accidente por el cableado, en caso de algun desastre natural permitira que la evacuación sea mas rápida y segura

 *Ilustración 3.1 2*  *Ilustración 3.1 3*	integra en la decoración de cualquier estancia de la casa. Por otro lado, otorgan seguridad, ya que mediante su utilización se evita que los cables queden sueltos, lo cual genera diversos riesgos: desde la posibilidad de enredarse los pies en ellos al andar y con la consecuente caída o daños en el sistema del cableado, o generar peligro inherente a cualquier cable conductor de electricidad, esto es, que la cobertura se dañe y quede expuesto un fragmento que pudiera afectar a una persona que lo tocara sin querer.	
 *Ilustración 4.1 1*	El no contar con ningun mobiliario especifico para acomodar o archivar ya sean papeles, cajas de folder con información, etc. Generará perdida de tiempo al no encontrar lo que se busca, debido al desorden, daños fisicos de la información contenida en los folder.	El uso de anaqueles permite que el desorden dentro de un departamento, ademas de producir mas espacio en el mismo.

 *Ilustración 5.1 1*  *Ilustración 5.1 2*  *Ilustración 5.1 3*	El no contar con un mobiliario para establecer los equipos y los access point tambien pueden generarse daños fisicos debido a que no tienen un lugar fijo, y el constante movimiento puede producir serios problemas en los equipos de computo, así como una mala estructuración de red dentro del departamento, de igual forma estar en el suelo provocará que las maquinas se llenen de polvo y sufran daños fisicos, teniendo como consecuencia daños fisicos	El uso de un mueble fijo donde se coloquen los equiposd de cómputo genera que no sufran daños fisicos al estar moviendolos, mas accesibilidad al realizar busqueda de información y evita que el polvo entre en contacto directo con el equipo.

CRONOGRAMA DE ACTIVIDADES

Nº	A C T I V I D A D	P/R	S E M A N A S														
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Recolección de información actual de la empresa.	P															
		R															
2	Elaboración de plan de auditoría.	P															
		R															
3	Elaboración de formatos de encuestas y entrevistas.	P															
		R															
4	Aplicación de encuestas y entrevistas al personal.	P															
		R															
5	Aplicación de entrevistas a encargados del personal.	P															
		R															
6	Evaluación del mobiliario y equipos.	P															
		R															
7	Identificación de riesgos.	P															
		R															
8	Verificación y recopilación de resultados.	P															
		R															
9	Realización de diagrama de Ishikawa.	P															
		R															
10	Identificación de causas del problema.	P															
		R															
11	Redacción de recomendaciones.	P															
		R															
12	Documentación de los hallazgos y anomalías encontradas.	P															
		R															
13	Entrega de informe final.	P															
		R															
14	Entrega de documentación de auditoría.	P															
		R															
15	Cierre de estadía.	P															
		R															

PLAN DE AUDITORÍA

Objetivos: Realizar una auditoría de seguridad física en la empresa automotriz GOMSA S.A de C.V, con el fin de identificar posibles vulnerabilidades existentes relacionadas a controles de seguridad, haciendo uso de la norma ISO 27002, con el propósito de implementar un modelo de seguridad y verificando la integridad de los activos.

- ✓ Evaluar y verificar los accesos a los sistemas de información para determinar si son adecuados y eficientes.
- ✓ Verificar el uso adecuado de la información proporcionada por la empresa (manuales).
- ✓ Evaluar los componentes físicos de la información de la empresa.
- ✓ Generar propuestas de solución y mejora que atiendan a las anomalías documentados en el diagnóstico de la auditoría.

Alcance: Se llevará a cabo una revisión de los procedimientos y el control adecuado para acceder a la información de la empresa, así como la revisión de los equipos de cómputo, mobiliario, las instalaciones y al personal.

Además de verificar los procedimientos ante contingencias como incendios, inundaciones, sabotajes, disturbios, etc. Así como la detección de amenazas no contempladas.

Criterios: COBIT, ***ISO/IEC*** 27002, revisión de manuales y documentos de la empresa.

Técnicas y Procedimientos: Plan de Auditoría

Auditor: *Jesús Daniel Enriquez Concepción*

Responsable Empresarial: *Ing. Miguel Ángel García Ramírez*

Responsable del Punto auditado:

Tipo de auditoria: Auditoría de Seguridad Física

Fecha:	**Sitio:** *Automotriz GOMSA S.A de C.V. de Córdoba*	**Hora:**

Reunión de apertura:	07 de enero de 2016	**Hora:**	9:00 a.m. – 2:00 p.m.
Reunión de cierre:	12 de febrero de 2016	**Hora:**	9:00 a.m. – 2:00 p.m.

Exclusiones: COBIT, ***ISO/IEC*** 27002

1. Establecimiento de los objetivos, alcances, misión, visión y creación del plan de auditoría.
2. Obtención de información a través de recursos necesarios para realizar la auditoría
3. Revisión de políticas de seguridad y otras normas involucradas
4. Evaluación de equipos, mobiliarios y procedimientos de la seguridad física
5. Evaluación de controles de acceso a la información
6. Evaluación de las redes físicas (Topología de red e infraestructura)
7. Evaluación de gestión de la información a Incidentes y desastres naturales
8. Detección de posibles amenazas
9. Listado de recomendaciones

Nº	ACTIVIDAD	REQUISITO POR AUDITAR (COBIT, ***ISO/IEC*** 27002)	AUDITADOS CARGO Y NOMBRE	AUDITOR	FECHA	HORA	Lugar
1	Establecimiento de objetivos, misión, visión y alcances.	**COBIT**		*Jesús Daniel Enriquez Concepción*			*Automotriz GOMSA S.A de C.V. de Córdoba*
2	Creación de encuestas y entrevistas.	***ISO/IEC*** 27002		*Jesús Daniel Enriquez Concepción*			
3	Aplicación de encuestas.			*Jesús Daniel Enriquez Concepción*			
4	Evaluación de los equipos y mobiliarios	***ISO/IEC*** 27002		*Jesús Daniel Enriquez Concepción*			

5	Evaluación de redes físicas	***ISO/IEC*** 27002		*Jesús Daniel Enriquez Concepción*			
6	Detección de posibles amenazas			*Jesús Daniel Enriquez Concepción*			
7	Obtención de resultados y recomendaciones	**COBIT**		*Jesús Daniel Enriquez Concepción*			

La iniciación, terminación y horarios de la auditoría se adecuarán de acuerdo con el desplazamiento de auditores

OBSERVACIONES:

Elaborado: *Jesús Daniel Enriquez Concepción* Revisado: _____ Aprobado: _____

Hoja controlada

Encuestador: *Jesús Daniel Enriquez Concepción*		
Responsable Empresarial: *Ing. Miguel Ángel García Ramírez*		
Nombre y cargo del entrevistado:		
Fecha:	**SITIO:** *Automotriz GOMSA S.A de C.V. de Córdoba*	**Hora:**

Instrucciones: Responda lo que se pide.

Nº	PREGUNTA	RESPUESTA	OBSERVACIONES	NORMA
1	¿El equipo de cómputo es adecuado para desempeñar su trabajo? ¿Por qué?			ISO/IEC 27002. Instalación y protección de equipos
2	¿Cuenta con algún mobiliario personal para su equipo de cómputo?			ISO/IEC 27002. Instalación y protección de equipos
3	¿Cree usted que el mobiliario, es el adecuado? ¿Por qué?			ISO/IEC 27002. Instalación y protección de equipos
4	En caso de que el mobiliario cuente con defectos. ¿Se reemplaza?			ISO/IEC 27002. Instalación y protección de equipos
5	¿Existe un reglamento que deba seguir el personal en caso de ser nuevo en la empresa? ¿Cual?			ISO/IEC 27002 Controles físicos de entrada
6	¿Existe algún tipo de formato o bitácora dónde se realicen registro del personal externo			ISO/IEC 27002 Controles físicos de entrada

	cuando hace uso de alguna maquina?			
7	¿Conoce usted si se maneja alguna norma dentro de su departamento? ¿Cuál es?			ISO/IEC 27002 Controles físicos de entrada
8	¿Está usted capacitado para reaccionar en caso de emergencia?			ISO/IEC 27002. Instalación y protección de equipos
9	¿Conoce alguna norma o políticas que se manejen en la empresa en cuestión de seguridad?			ISO/IEC 27002 Controles físicos de entrada
10	¿Se le permite a usted introducir equipos externos a la empresa (laptops)?			ISO/IEC 27002. Instalación y protección de equipos
11	¿Las instalaciones cuentan con detectores de humo, en caso de incendios?			ISO/IEC 27002 Protección contra amenazas
12	¿Existe algún extintor dentro de su área de trabajo? ¿Cuantos?			ISO/IEC 27002 Controles físicos de entrada
13	¿En caso de fallo de algún equipo, este se sustituye?			ISO/IEC 27002 Suministro eléctrico
14	¿Se tienen bitácoras ya sean digitales o a papel, de fallos de los equipos? Cuál es el proceso.			ISO/IEC 27002 Suministro eléctrico
15	¿Se realiza mantenimiento a los equipos frecuentemente?			ISO/IEC 27002 Suministro eléctrico

16	¿Se realizan respaldo de información en caso de desastres naturales?			ISO/IEC 27002 Protección contra amenazas externos y del entorno
17	Respalda su información frecuentemente, siempre o casi nunca.			ISO/IEC 27002 Controles físicos de entrada
18	¿Se cuenta con manual de usuario sobre el uso de los equipos?			ISO/IEC 27002 Controles físicos de entrada
19	¿Cada equipo de cómputo dentro de su área de trabajo cuenta con contraseña personal o es abierta para cualquier persona?			ISO/IEC 27002 Utilización y seguridad de los soportes de información
20	¿Existe restricción para almacenar información como USB, u otro dispositivo? ¿Por qué?			ISO/IEC 27002 Protección contra amenazas externos y del entorno
21	¿Se realiza alguna medida de seguridad en caso de extravió de información importante?			ISO/IEC 27002 Protección contra amenazas externos y del entorno
24	¿En qué periodo de tiempo desecha los archivos basura de su equipo de cómputo?			ISO/IEC 27002 Protección contra amenazas externos y del entorno
25	¿Existe alguna política para la descarga de software en los equipos?			ISO/IEC 27002 Protección contra amenazas externos y del entorno
26	¿Se cuenta con software o software´s exclusivo de la			ISO/IEC 27002 Utilización y seguridad de los

	empresa? Mencione nombre o nombres,			soportes de información
27	¿Se realizan auditorias frecuentemente, siempre, poco o rara vez?			ISO/IEC 27002 Seguridad de la documentación
28	¿Se hace mención del objetivo de la auditoria?			ISO/IEC 27002 Eliminación de soporte
29	¿Se realizan auditorias con respecto a la seguridad?			ISO/IEC 27002 Utilización y seguridad de los soportes de información

Elaborado: *Jesús Daniel Enriquez Concepción* Revisado: _____ Aprobado: _____

Hoja controlada

Encuestador: *Jesús Daniel Enriquez Concepción*		
Responsable Empresarial: *Ing. Miguel Ángel García Ramírez*		
Nombre y cargo del encuestado:		
Fecha:	**SITIO:** *Automotriz GOMSA S.A de C.V. de Córdoba*	**Hora:**

Instrucciones: Marque con una x según corresponda su respuesta.

Nº	PREGUNTA	CUMPLE		OBSERVACIONES
		SI	NO	
1	¿La ubicación del centro de cómputo está seguro de inundaciones, robo o cualquier otra situación que pueda poner en peligro los equipos?			
2	¿En el área de cómputo se cuentan con armarios ignífugos (anti fuegos)?			
3	¿Dentro del área existen materiales que sean inflamables, o puedan causar algún daño a los equipos?			
4	¿Existe espacio suficiente para los equipos?			
5	¿Es adecuada la iluminación dentro del área?			
6	¿La temperatura en la que trabajan los equipos es la adecuada para su durabilidad?			

7	¿Dentro del área de cómputo, existen equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, UPS, generadores de energía?			
8	¿Existe procedimiento de mantenimiento por parte de la empresa, en el centro de cómputo?			
9	¿Existe una sala o edificio donde se encuentre alojado el servidor?			
10	¿Los cables están bien instalados dentro del centro de cómputo, es decir si se encuentran dentro de canales o paneles?			
11	¿Los equipos cuentan con antivirus?			
12	¿Se lleva un registro de incidencias de virus en cada equipo?			
13	¿El cableado de red de los equipos se encuentra etiquetado?			
14	¿Se cuenta con un sistema puesta a tierra para los equipos de cómputo en caso de descargas eléctricas?			
15	¿Los antivirus instalados son adecuados para la eliminación de virus en los equipos?			
16	¿Existen políticas para la seguridad de la información en los equipos de cómputo de cada departamento?			
17	¿Dichas políticas están documentadas?			
18	¿El acceso a los equipos del centro de cómputo, cuentan con medidas de seguridad para acceder a ellos?			
19	¿Se tienen implementadas dichas contraseñas en cada equipo?			
20	¿Se emplean cuentas de usuario para cada terminal en cada departamento?			
21	¿Cuentan con inventario o inventarios de los equipos de cómputo?			
22	¿Se realiza un chequeo frecuente del inventario de los equipos?			
23	¿Se cuenta con instalación eléctrica específicamente para los equipos de cómputo?			
24	¿Se tienen bitácoras para el acceso del personal a los equipos de cómputo?			
25	¿Los equipos de cómputos se encuentran conectados a UPS o algún tipo de regulador eléctrico?			

26	¿Existen normas o políticas para el acceso del personal externo a la empresa?			
27	¿Dichas normas o políticas se tienen documentadas?			
28	¿Cuentan con extintores, sistema contra incendios donde se encuentran los equipos?			
29	¿Cuentan con alguna topología de red?			
30	¿En caso de que el nuevo personal de la empresa acceda al centro de cómputo, se le facilita usando los manuales (Técnico – Usuario si se cuenta)?			
31	¿La información de los equipos se encuentra a salvo de terremotos, inundaciones, incendios o algún otro tipo de desastre natural?			

Elaborado: *Jesús Daniel Enriquez Concepción* Revisado: _____ Aprobado: _____

Hoja controlada

CAPÍTULO 5

5.1 Recopilación y evaluación de resultados

5.1.1 Aplicación de la norma ISO 27002

De acuerdo a los resultados obtenidos de las evaluaciones que se realizaron dentro de la empresa, se observa que no se cumplen en su totalidad con los requisitos que se establecen en la norma ISO 270002, así mismo, que cada departamento desconoce los reglamentos de seguridad física establecidos por la misma.

La aplicación de esta norma en la empresa es muy útil, debido a que la norma establece medidas de seguridad tanto lógicas como físicas para respaldar y resguardar la información importante que se maneja día con día en cualquier tipo de empresa, nos explica sobre la protección física de los equipos ante cualquier amenaza, ya sea desde conectar un dispositivo portátil hasta el acceso de personal no autorizado por la empresa, esto con el fin de evitar riesgos que generen perdida de información o produzcan perdidas físicas y costosas.

De igual forma la norma nos explica sobre una adecuada infraestructura para evitar daños físicos del cableado y tener bien estructurada la red. El fin de difundir esta norma en la empresa automotriz GOMSA es por el motivo de los resultados obtenidos y por las pruebas que se obtuvieron a lo largo del desarrollo de la auditoría. A continuación se da a conocer la importancia de la aplicación de la norma ISO 27002:

1. **Seguridad física (protección física) del sistema informático y prevención de accesos no autorizados a la información y daños a los mismos.**

    - Se dan a conocer las amenazas de carácter físico y ambiental a las que pueden estar sometidas las infraestructuras físicas del Sistema Informático, así como las salvaguardas e implementar para disminuir la probabilidad de materialización de dichas amenazas o disminuir su impacto si éstas se llegan a materializar.

2. **Control y administración de acceso de usuarios, autenticación, criptografía, control de acceso a la red, a las máquinas y las aplicaciones, detección de accesos no autorizados y el registro de eventos.**

    - La norma ISO 27002 presenta la necesidad de proteger de forma lógica los datos manejados en el ordenador y la red, ante las amenazas que en diversas formas y fines que se presentan. Se muestran las diferentes técnicas de identificación y autenticación de las entidades que acceden a la información para que el acceso se realice, exclusivamente, por aquellas autorizadas y se eviten los accesos indebidos. Proporciona los conceptos básicos de la criptografía, como herramienta de protección lógica, para entender los mecanismos de protección de datos hoy en uso.

3. **La Seguridad en las nuevas arquitecturas de Sistemas**

    - Se muestran los principales problemas de seguridad existentes en las nuevas arquitecturas de sistemas como Cloud Computing y virtualización, así como en los sistemas operativos más utilizados, las políticas y mecanismos empleados para resolver y mitigar dichos problemas.

5.1.2 Aplicación del diagrama causa – efecto (Ishikawa).

Uso del diagrama de causa – efecto (Ishikawa).

El diagrama causa-efecto es una forma de organizar y representar las diferentes teorías propuestas sobre las causas de un problema. Se conoce también como diagrama de causa-efecto y se utiliza en las fases de diagnóstico y solución de la causa. Su objetivo es identificar y cuantificar las causas de un problema, y encontrar en forma metódica las causas de un problema, además de radicar en busca de las diferentes causas que afectan el problema bajo análisis, evita el error de buscar de manera directa las soluciones sin cuestionar las cuales son las verdaderas causas.

5.1.3 Fortalezas del diagrama causa - efecto. Beneficios

- Ayuda a encontrar y a considerar todas las causas posibles del problema, más que apenas aquellas que son las más obvias.
- Ayuda a determinar las causas raíz de un problema o calidad característica, de una manera estructurada.
- Anima la participación grupal y utiliza el conocimiento del proceso que tiene el grupo.
- Ayuda a focalizarse en las causas del tema sin caer en quejas y discusiones irrelevantes.
- Aumenta el conocimiento sobre el proceso ayudando a todos a aprender más sobre los factores referentes a su trabajo y cómo éstos se relacionan.
- Identifica las áreas para el estudio adicional donde hay una carencia de información suficiente.

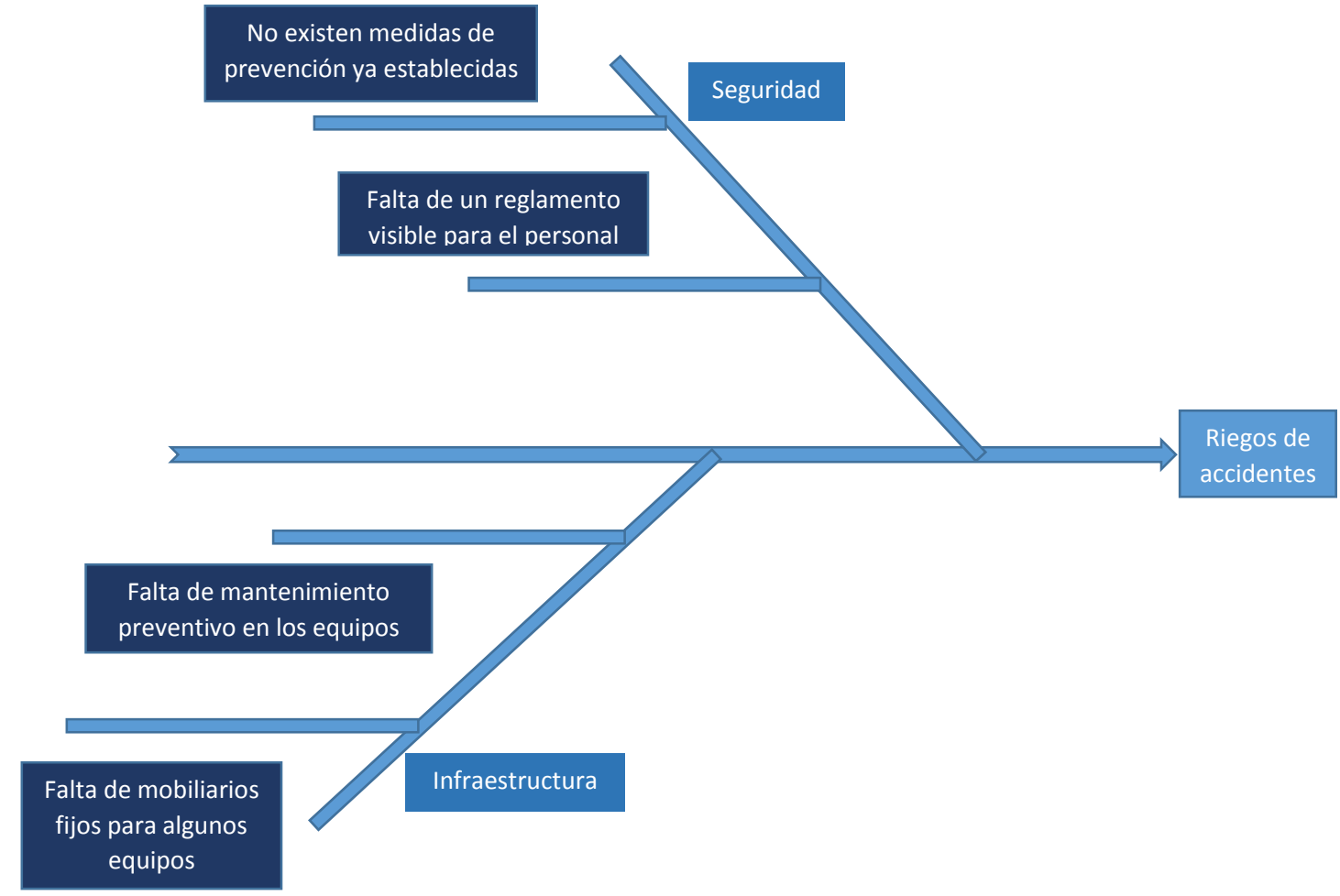


Diagrama Ishikawa 1.1 1

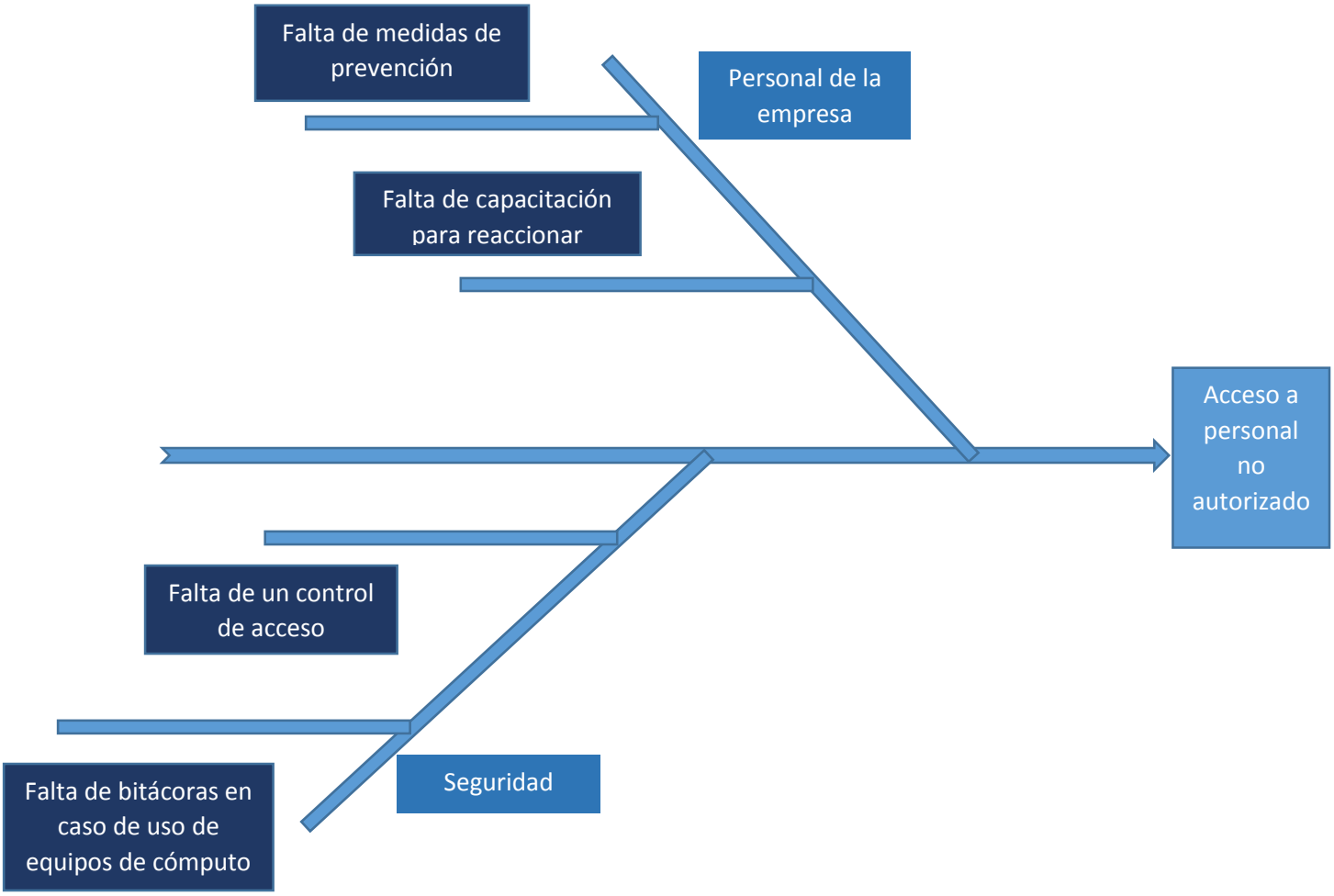


Diagrama Ishikawa 1.1 2

5.1.4 Identificación de causas del problema.

Equipos de cómputo de la empresa

1) No cumplen con un plan de mantenimiento de los equipos de cómputo, ya sea mantenimiento preventivo o correctivo.
2) Falta de medidas de seguridad o normas dentro de cada departamento, para el cuidado adecuado de los equipos de cómputo.
3) La topología de red que se estableció dentro de la empresa, es la adecuada para el personal que utiliza diariamente los equipos de cómputo, el problema consiste en una mala infraestructura.

4) No se utilizan reguladores o tomacorrientes de energía eléctrica suficientes para los equipos de cómputo de la empresa.
5) Fallas de hardware por falta de mantenimiento o por descuido de los empleados
6) Problemas en software`s exclusivos de la empresa
7) Se debe contar con un cuarto exclusivo para el servidor aunque sea improvisto, esto para evitar más riesgos a futuros
8) Implementación de canaletas para protección de cables.
9) Tener en orden en cada espacio y en su lugar el material que se utiliza en el departamento
10) Tener una mayor actualización en los antivirus de las computadoras que se tiene en cada departamento

Accesos no autorizados

1) No existen bitácoras de entrada y salida, del personal externo que ingresa a la empresa y a los equipos de cómputo en especial.
2) No existe ningún reglamento o normas por departamento, que dé a conocer las posibles amenazas que pueden ser causadas por personal externo, esto puede ser tanto robo de información o perdida de equipos tanto físico, como lógico.
3) El personal en general no conoce ningún tipo de norma o estándar que prevenga los posibles riesgos que existen por acceso a personal no autorizado o externo a la empresa.
4) Se debe contar con un reglamento visible para todos los empleados ya sean externos o internos que acceden a la empresa.

Posibles riesgos o amenazas físicas dentro de la empresa

1) Poco espacio entre los equipos de cómputo, esto solo sucede con algunos equipos de empleados, debido al área en donde desempeñan su trabajo diario.
2) Cableado expuesto ya sea de red o eléctrica
3) Debido a que los empleados desconocen que es un mantenimiento preventivo, los equipos de cómputo cuentan con poca limpieza
4) El personal no tiene conocimiento suficiente sobre el tema de medidas de seguridad físicas con respecto a la información

5) No existen normas o estándares sobre la seguridad física y de la información.
6) No existen medidas de seguridad de la información, como es el robo de información o sabotajes por personal externo
7) No se tienen extinguidores suficientes por departamento en caso de incendios
8) Capacitación insuficiente a todo el personal sobre terremotos, incendios, o algún otro tipo de desastre natural.
9) Se debe contar con medidas de seguridad en caso de desastres naturales

5.1.5 Documentación de hallazgos y anomalías encontradas

Tabla 2.1 1

Tipo de auditoría	Seguridad Física basada en la Norma ISO 27002
Nombre del componente	Acceso del personal a los sistemas de cómputo, tanto software como hardware, para acceder a la información.
Hallazgo	La información importante de la empresa se encuentra respaldada en un servidor con el motivo de asegurar la información y se cuenta con contraseñas, para evitar el acceso fácil del personal externo a la información, pero, no se tienen un control de los empleados que pertenecen a la empresa que acceden a dicha información.
Anomalía	Falta de conocimiento por parte de los empleados, de las consecuencias graves a la empresa el acceso de personal externo

Tabla 2.1 2

Tipo de auditoría	Seguridad Física basada en la Norma ISO 27002
Nombre del área	Control de acceso de los empleados a los equipos de cómputo
Hallazgo	Solo los empleados del área o de cada departamento tienen acceso a los equipos de cómputo
Anomalía	No se cuenta con una bitácora en caso de que exista una anomalía ya sea de hardware o software.

Tabla 2.1 3

Tipo de auditoría	Seguridad Física basada en la Norma ISO 27002
Nombre del área	Informes de accesos y visitas a las instalaciones
Hallazgo	No existe ningún control tangible de quienes entran o salen del departamento, siempre y cuando estos accedan a la información de dicho departamento, y el control que se tiene al acceso es solamente verbal.
Anomalía	Se puede generar pérdidas físicas y lógicas de la información que se tiene en cada departamento por el acceso de personal externo y no contar con un control adecuado de entradas y salidas.

Tabla 2.1 4

Tipo de auditoría	Seguridad Física basada en la Norma ISO 27002
Nombre del área	Revisión de la red (Factor ambiental, físico y humano)
Hallazgo	El cableado en su mayoría UTP categoría 5e UL & ISO 9001, se encuentra expuesto en algunos departamentos de la empresa, es decir no cuentan con canaletas.
Anomalía	El riesgo de que surja un accidente por tener un cable expuesto es muy probable, debido a que si existe un desastre natural, al momento de evacuar puede generar tropiezos o incluso caídas graves a los empleados, además de que el cable no está protegido y puede deteriorarse más pronto, y se recomienda mantener las conexiones y equipos de telecomunicaciones a más de 10 metros de distancia, esto con el fin de cumplir con la norma de la ISO.

Tabla 2.1 5

Tipo de auditoría	Seguridad Física basada en la Norma ISO 27002
Nombre del área	Plan de contingencias
Hallazgo	Carecen de planes de contingencias de operaciones y planes en caso de fallo total o parcial de sus sistemas. Como se puede observar esto puede ser un punto de debilidad de la empresa porque mediante el plan de contingencia se asegura que la empresa seguirá ofreciendo su servicio sin importar las condiciones.
Anomalía	Si no se cuenta con un plan de contingencia los encargados del personal no será informado de las tareas a realizar, que realizar en caso de amenazas, y se perderá el control y el orden

Tabla 2.1 6

Tipo de auditoría	Seguridad Física basada en la Norma ISO 27002
Nombre del componente	Plan de mantenimiento de hardware y software
Hallazgo	No se encuentra establecido un plan sólido de mantenimiento de hardware, esto debería ser de forma preventiva y correctiva, así como de forma correctiva el software
Anomalía	Si no se tiene un plan de mantenimiento, la durabilidad de los equipos minorizará, teniendo como consecuencias perdida de información, eh incluso fallo de los equipos

5.1.6 Recomendaciones

- Prevención contra desastres naturales y actos mal intencionados.
- Ventilación adecuada de los equipos.
- Implementación de canaletas para la protección de los cables.
- Organización y planeación del mantenimiento de los equipos.
- Se recomienda que se establezca un control del acceso del personal externo a departamentos, es decir contar con una bitácora ya sea a papel o digital para tener el control del acceso.
- Se recomienda mantener una lista, que ayude en el control de quien accede a los equipos de cómputo, esto para evitar que existan daños de hardware y software de los equipos.
- Se recomienda que el espacio donde los equipos de cómputo se encuentran alojados sean libres de papeles o de líquidos que causen daños físicos a los equipos.
- Se recomienda generar un plan de mantenimiento, esto con el fin de mantener los equipos a salvo de polvo o cualquier otro tipo de factor que dañe físicamente el equipo, se recomienda que se lleve a cabo el mantenimiento preventivo.
- Se recomienda contar con un plan de contingencia, en caso de fallas parciales o totales, esto con el fin de que la empresa demuestre que si esto sucede puede recuperarse y reanudar sus operaciones sin importar los acontecimientos
- Se recomienda a la empresa diagramar y esquematizar el software o software´s que posee, así mismo su red en uso, esto con el fin de visualizar de forma concreta y rápida los servicios utilizados por la empresa
- En algunos departamentos el espacio que se tiene exclusivo para los equipos de cómputo es mínima, o no se cuenta con mobiliario adecuado para colocar los reguladores de corriente, por lo que se colocan los equipos sobre los mismos. Esto puede generar o producir efectos secundarios sobre los equipos.

5.1.6 Informe final

AUDITORIA DE SEGURIDAD FÍSICA

INSTITUCIÓN

AGENCIA AUTOMOTRIZ GOMSA S.A. DE C.V.

AUDITOR

JESÚS DANIEL ENRIQUEZ CONCEPCIÓN

FECHA DE EJECUCIÓN

DEL 11 DE ENERO AL 11 DE ABRIL DE 2016

Introducción

En el informe final de esta auditoría se presenta la consolidación de las investigaciones realizadas en la empresa automotriz GOMSA S.A. de C.V. de la ciudad de Córdoba, Veracruz, analizando los departamentos que cuentan con equipos de cómputo.

Es muy importante saber que, aunque la empresa sea la más segura desde punto de vista de ataques externos, la seguridad de la misma será nula, si no se ha previsto como combatir un incendio o cualquier tipo de desastre natural, además de no haber establecido normas o políticas de seguridad para una recuperación inmediata.

La seguridad física es uno de los aspectos importantes dentro de cualquier organización, ya sea pequeña, mediana o grande. Si bien algunos de los aspectos de seguridad física básicos se prevén, otros, como la detección de atacantes internos dentro de una empresa u organización, ese aspecto, no.

Así, la seguridad física consiste en la "aplicación de barreras físicas y procedimientos de control, como medida de prevención y contramedidas de amenazas a los recursos e información confidencial". Se refiere en particular a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo, también es implementado para proteger el hardware y medio de almacenamientos de datos.

El aporte consiste en la descripción de los problemas encontrados, causas que lo originaron, repercusiones que pueden ocasionar daños en la empresa y alternativas para solucionar dichos problemas, de igual forma se pretende que sean analizados y evaluados en cuanto a la conveniencia la implementación de las recomendaciones establecidas, las cuales son vertidas de manera sencilla, y los criterios establecidos según la norma ISO 27002.

Córdoba, Veracruz a 7 de abril de 2016

Ing. Miguel Ángel García Ramírez
Asesor industrial
Automotriz GOMSA S.A. de C. V.
Presente

Se informa por este medio nuestro deseo de éxitos en las labores que a diario realizan, en beneficio de la población que demanda sus servicios.

Me dirijo a usted para agradecer la oportunidad de llevar a cabo la auditoría con respecto a la seguridad física, así mismo de remitir el informe final de la auditoría realizada en la agencia automotriz GOMSA S.A. de C. V. Detallando los aspectos que se tomaron en cuenta para evaluar el área de informática, así como los problemas detectados en cada una de ellas, las causas que las originan, las repercusiones que pueden tener en la organización, posibles alternativas de solución y las recomendaciones que al realizar la auditoria se pretende que se lleven a cabo, con el fin de corregir las desviaciones y lograr así que los equipos de cómputo cumplan eficientemente los objetivos para los cuales fueron implementados.

Gracias por la colaboración proporcionada para la ejecución de la auditoría de seguridad física.

Auditor
Jesús Daniel Enriquez Concepción

CAPÍTULO 6

6.1 Conclusiones

El presente trabajo de auditoría ha dado a conocer la manifestación de diversos problemas a los cuales se les han planteado recomendaciones, en consecuencia, el personal de la institución deberán conocer las políticas y medidas de seguridad que debe existir para el cuidado de la información, así como el uso de los equipos de cómputo, mantenimiento, confidencialidad, respaldo y almacenamiento de información.

En términos generales y de acuerdo a lo manifestado por los encargados y empleados de cada área, los equipos de cómputo son los adecuados para llevar a cabo sus labores cotidianas. La agencia necesita brindar servicio de mantenimiento preventivo y correctivo a los equipos de cómputo, tanto nivel hardware como software. El uso adecuado de canaletas para proteger los cables ya sean para obtener energía o red, deben ser implementadas, con el fin de mantener la seguridad del cable y la de los empleados.

De manera general la seguridad física basada en la norma ISO 27002, nos ayuda a evaluar tanto el entorno de donde se encuentran los equipos, evaluación del hardware y medidas de seguridad de información a nivel software, es decir el acceso que tiene la información con el entorno.

CAPÍTULO 7

7.1 Referencias

© Ministerio de Educación, C. y. (19 de Enero de 2010). *Monográfico ISO 27002*. Obtenido de http://recursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

Carvajal, F. M. (7 de Marzo de 2011). *LA PLANEACION*. Obtenido de http://laplaneacion2011.blogspot.mx/2011/03/la-planeacion.html

COBIT. (10 de mayo de 2007). *COBIT: MODELO PARA AUDITORIA Y CONTROL DE SISTEMAS DE INFORMACIÓN*. Obtenido de http://www.hacienda.go.cr/cifh/sidovih/spaw2/uploads/images/file/COBIT%20audit%20y%20ctrol%20sists%20inf.pdf

contables, A. (12 de Marzo de 2014). *Auditorias contables*. Obtenido de http://www.auditoriascontablescr.com/auditorias.html

CONTACADEMICA. (12 de Febrero de 2015). *Metodología*. Obtenido de http://www.academica.mx/blogs/contacademica?page=1

Copyright © 2003-2016 Farlex, I. (3 de Septiembre de 2011). *Plan*. Obtenido de http://es.thefreedictionary.com/plan

Copyright © 2003-2016 Farlex, I. (12 de Junio de 2011). *Programa*. Obtenido de http://es.thefreedictionary.com/programa

de, C. (14 de Octubre de 2001). *Concepto de Entrevista*. Obtenido de http://concepto.de/entrevista/

futuro, N. (2 de Abril de 2002). *Auditoría de sistemas*. Obtenido de Los mecanismos de seguridad física deben resguardar de amenazas producidas tanto por el hombre como por la naturaleza. Básicamente, las amenazas físicas que pueden poner en riesgo un sistema informático son:

Geografía, I. N. (14 de Julio de 2010). *Diseño de Cuestionarios*. Obtenido de http://www.inegi.org.mx/prod_serv/contenidos/espanol/bvinegi/productos/metodologias/varios/Dise%C3%B1o_Cuest.pdf

Investigación, I. F. (23 de Agosto de 2004). *Tipos de métodos*. Obtenido de https://sites.google.com/site/itslfundamentosdeinvestigacion/b-organizacion-de-los-contenidos-lecturas-y-recursos/2-3-tipos-de-metodos-inductivo-deductivo-analitico-sintetico-comparativo-dialectico-entre-otros

Roldán, C. S. (25 de Febrero de 2013). *¿Qué es una Auditoría Informática?* Obtenido de https://www.codejobs.biz/es/blog/2013/02/25/que-es-una-auditoria-informatica

CAPÍTULO 8

8.1 Anexos

GM CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 1 de 3

Encuestador: *Jesús Daniel Enríquez Concepción*

Responsable Empresarial: *Ing. Miguel Ángel García Ramírez*

Nombre y cargo del entrevistado: Isaba Martinez Rayon Administrador Garantias.

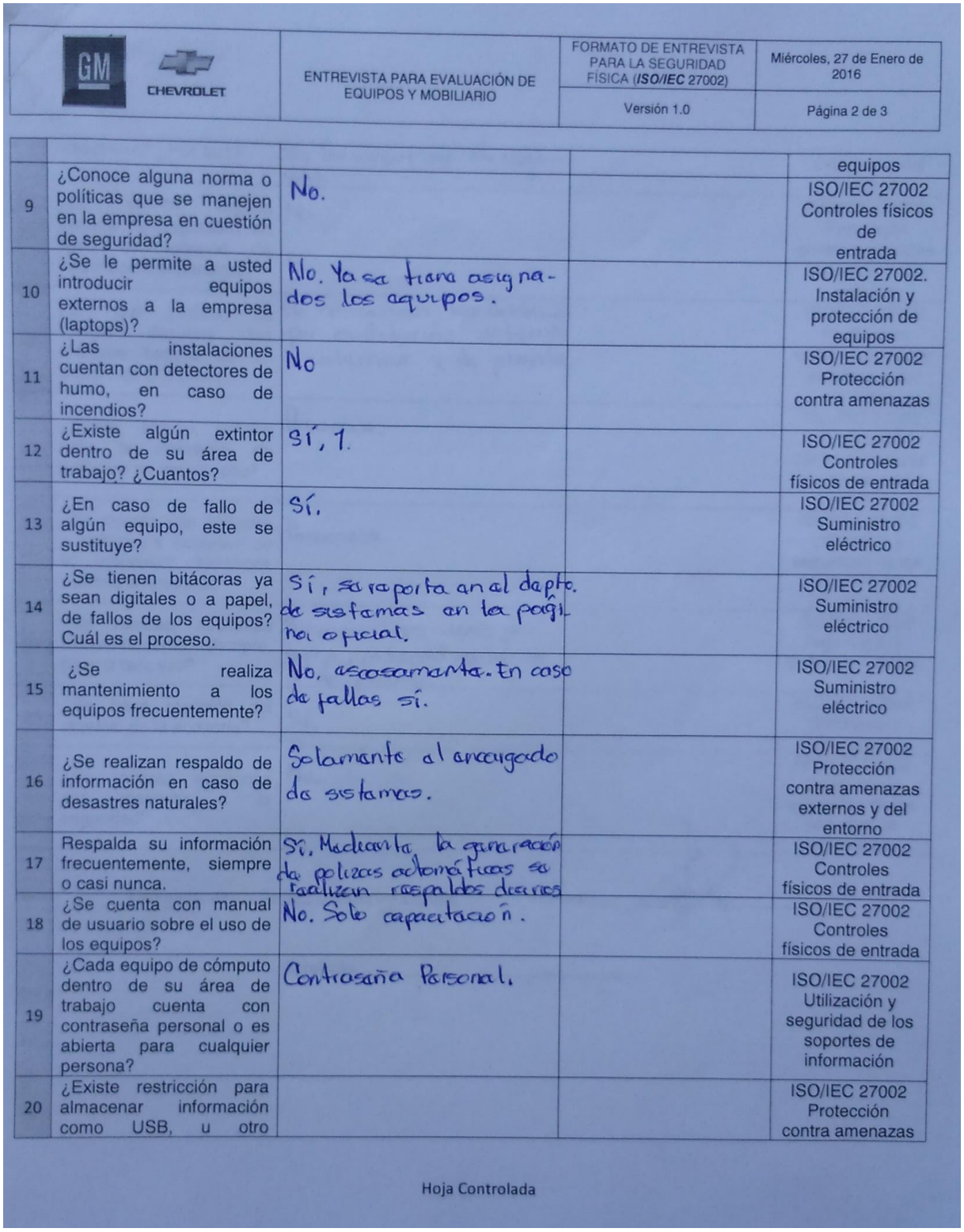
Fecha:	**SITIO:** *Automotriz GOMSA S.A de C.V. de Córdoba*	**Hora:**

Instrucciones: Responda lo que se pide.

Nº	PREGUNTA	RESPUESTA	OBSERVACIONES	NORMA
1	¿El equipo de cómputo es adecuado para desempeñar su trabajo? ¿Por qué?	Sí, Porque cuenta con todas las herramientas necesarias.		ISO/IEC 27002. Instalación y protección de equipos
2	¿Cuenta con algún mobiliario personal para su equipo de cómputo?	Sí.		ISO/IEC 27002. Instalación y protección de equipos
3	¿Cree usted que el mobiliario, es el adecuado? ¿Por qué?	Sí, Para sus actividades es adecuado		ISO/IEC 27002. Instalación y protección de equipos
4	En caso de que el mobiliario cuente con defectos. ¿Se reemplaza?	Sí.		ISO/IEC 27002. Instalación y protección de equipos
5	¿Existe un reglamento que deba seguir el personal en caso de ser nuevo en la empresa? ¿Cual?	Sí, existen politicas de la amprasa		ISO/IEC 27002 Controles físicos de entrada
6	¿Existe algún tipo de formato o bitácora dónde se realicen registro del personal externo cuando hace uso de alguna maquina?	No		ISO/IEC 27002 Controles físicos de entrada
7	¿Conoce usted si se maneja alguna norma dentro de su departamento? ¿Cuál es?	No.		ISO/IEC 27002 Controles físicos de entrada
8	¿Está usted capacitado para reaccionar en caso de emergencia?	Sí.		ISO/IEC 27002. Instalación y protección de

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 1

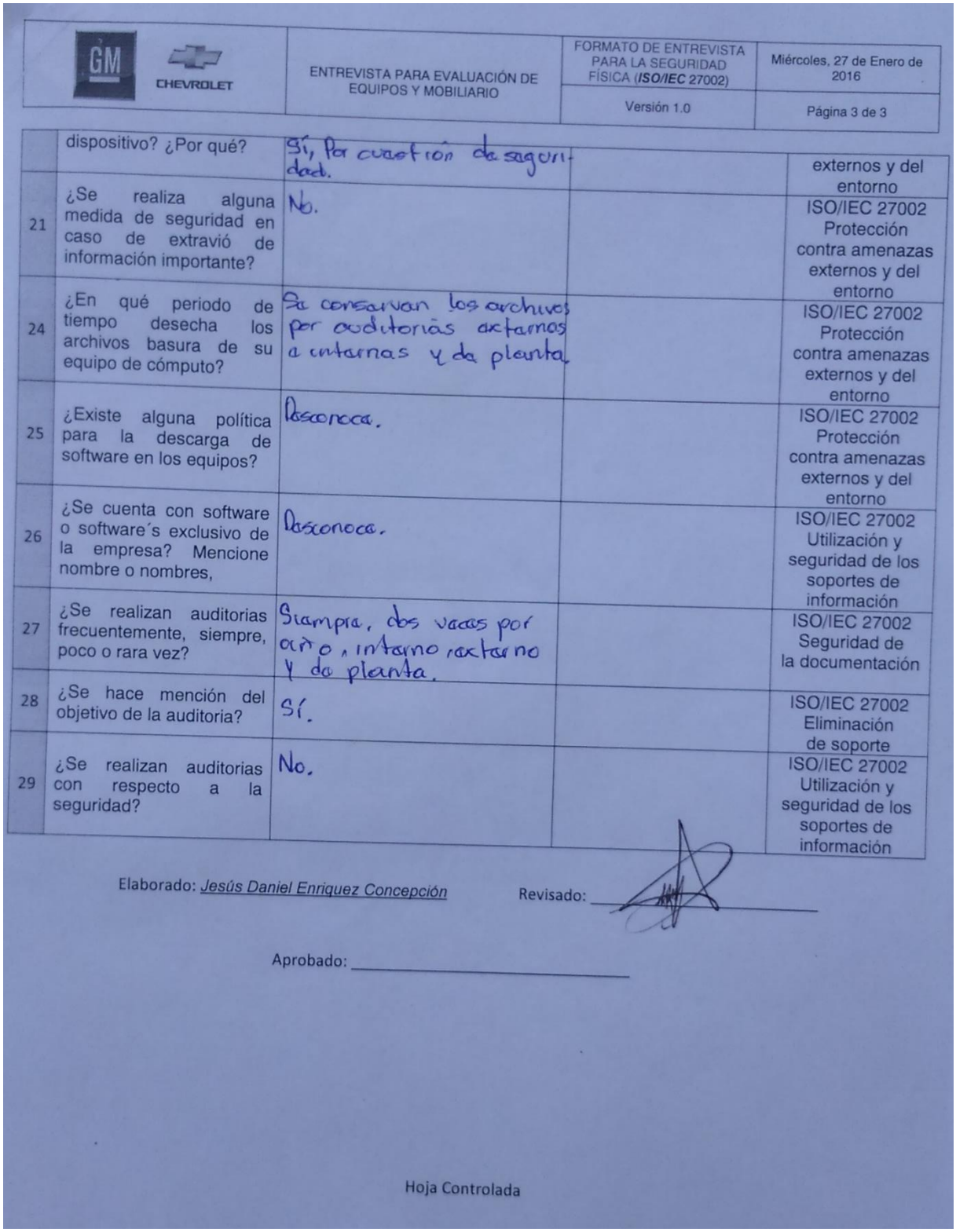


GM / CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 2 de 3

				equipos
9	¿Conoce alguna norma o políticas que se manejen en la empresa en cuestión de seguridad?	No.		ISO/IEC 27002 Controles físicos de entrada
10	¿Se le permite a usted introducir equipos externos a la empresa (laptops)?	No. Ya se tiene asignados los equipos.		ISO/IEC 27002. Instalación y protección de equipos
11	¿Las instalaciones cuentan con detectores de humo, en caso de incendios?	No		ISO/IEC 27002 Protección contra amenazas
12	¿Existe algún extintor dentro de su área de trabajo? ¿Cuantos?	Sí, 1.		ISO/IEC 27002 Controles físicos de entrada
13	¿En caso de fallo de algún equipo, este se sustituye?	Sí.		ISO/IEC 27002 Suministro eléctrico
14	¿Se tienen bitácoras ya sean digitales o a papel, de fallos de los equipos? Cuál es el proceso.	Sí, se reporta en el depto. de sistemas en la página oficial.		ISO/IEC 27002 Suministro eléctrico
15	¿Se realiza mantenimiento a los equipos frecuentemente?	No, ocasionalmente. En caso de fallas sí.		ISO/IEC 27002 Suministro eléctrico
16	¿Se realizan respaldo de información en caso de desastres naturales?	Solamente al encargado de sistemas.		ISO/IEC 27002 Protección contra amenazas externos y del entorno
17	Respalda su información frecuentemente, siempre o casi nunca.	Sí. Mediante la generación de polizas automáticas se realizan respaldos diarios		ISO/IEC 27002 Controles físicos de entrada
18	¿Se cuenta con manual de usuario sobre el uso de los equipos?	No. Solo capacitación.		ISO/IEC 27002 Controles físicos de entrada
19	¿Cada equipo de cómputo dentro de su área de trabajo cuenta con contraseña personal o es abierta para cualquier persona?	Contraseña Personal.		ISO/IEC 27002 Utilización y seguridad de los soportes de información
20	¿Existe restricción para almacenar información como USB, u otro			ISO/IEC 27002 Protección contra amenazas

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 2



GM CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 3 de 3

	dispositivo? ¿Por qué?	Sí, Por cuestión de seguridad.		externos y del entorno
21	¿Se realiza alguna medida de seguridad en caso de extravió de información importante?	No.		ISO/IEC 27002 Protección contra amenazas externos y del entorno
24	¿En qué periodo de tiempo desecha los archivos basura de su equipo de cómputo?	Se conservan los archivos por auditorías externas e internas y de planta.		ISO/IEC 27002 Protección contra amenazas externos y del entorno
25	¿Existe alguna política para la descarga de software en los equipos?	Desconoce.		ISO/IEC 27002 Protección contra amenazas externos y del entorno
26	¿Se cuenta con software o software´s exclusivo de la empresa? Mencione nombre o nombres,	Desconoce.		ISO/IEC 27002 Utilización y seguridad de los soportes de información
27	¿Se realizan auditorias frecuentemente, siempre, poco o rara vez?	Siempre, dos veces por año, interno, externo y de planta.		ISO/IEC 27002 Seguridad de la documentación
28	¿Se hace mención del objetivo de la auditoria?	Sí.		ISO/IEC 27002 Eliminación de soporte
29	¿Se realizan auditorias con respecto a la seguridad?	No.		ISO/IEC 27002 Utilización y seguridad de los soportes de información

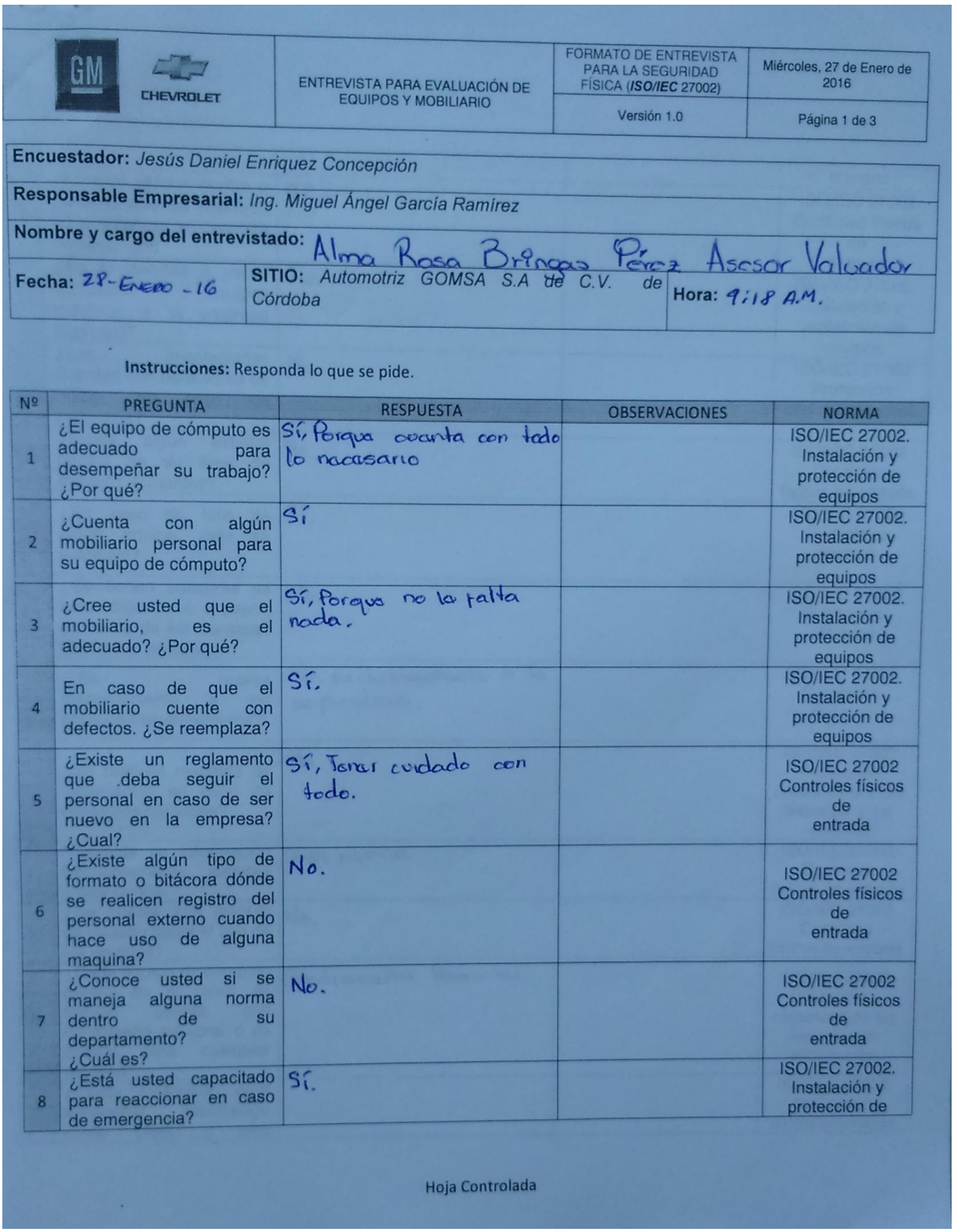
Elaborado: *Jesús Daniel Enriquez Concepción*

Revisado: _____

Aprobado: _____

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 3



GM CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 1 de 3

Encuestador: *Jesús Daniel Enriquez Concepción*

Responsable Empresarial: *Ing. Miguel Ángel García Ramírez*

Nombre y cargo del entrevistado: Alma Rosa Bringas Pérez Asesor Valuador

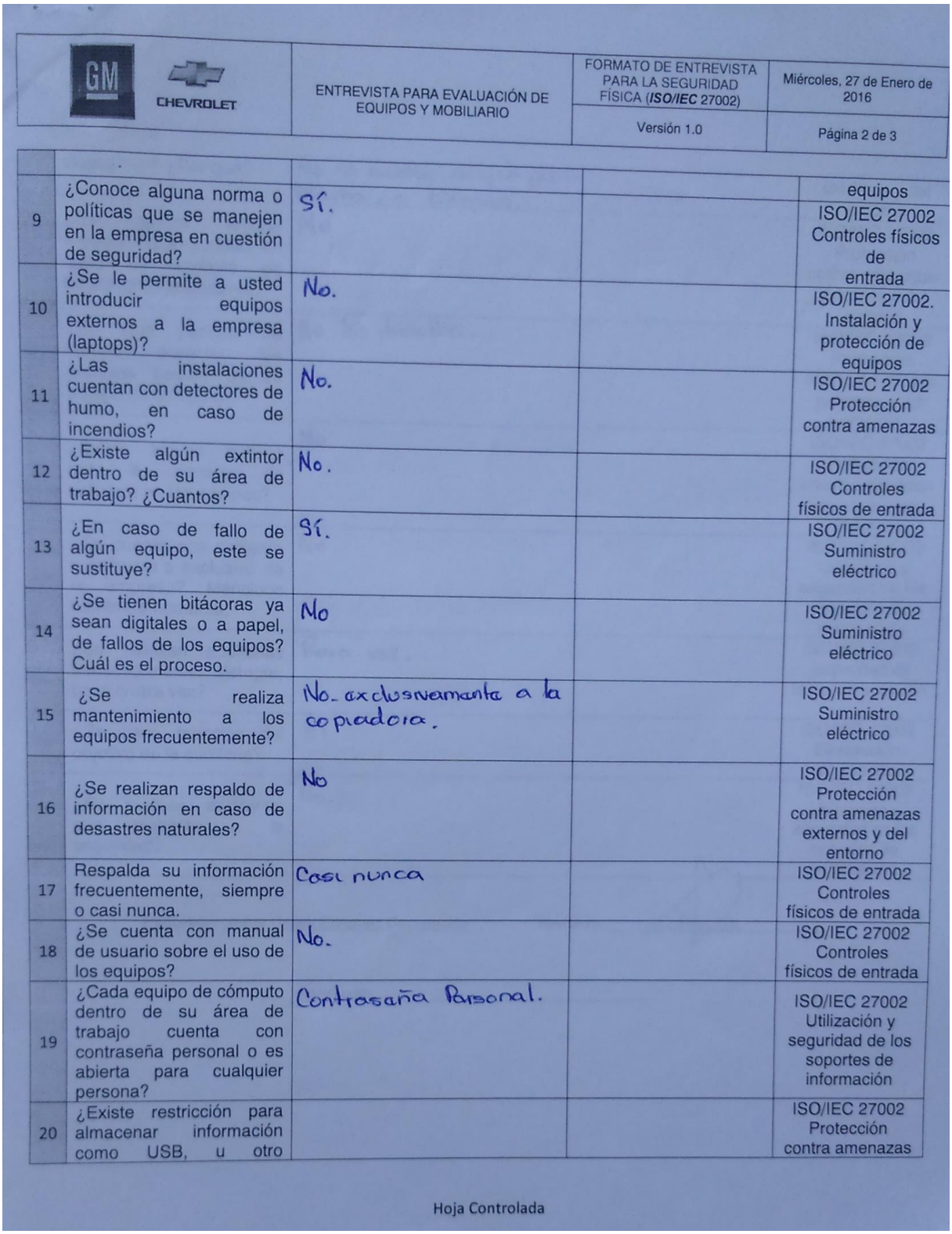
Fecha: 28-Enero-16	**SITIO:** *Automotriz GOMSA S.A de C.V. de Córdoba*	**Hora:** 9:18 A.M.

Instrucciones: Responda lo que se pide.

Nº	PREGUNTA	RESPUESTA	OBSERVACIONES	NORMA
1	¿El equipo de cómputo es adecuado para desempeñar su trabajo? ¿Por qué?	Sí, Porque cuenta con todo lo nacasario		ISO/IEC 27002. Instalación y protección de equipos
2	¿Cuenta con algún mobiliario personal para su equipo de cómputo?	Sí		ISO/IEC 27002. Instalación y protección de equipos
3	¿Cree usted que el mobiliario, es el adecuado? ¿Por qué?	Sí, Porque no le falta nada.		ISO/IEC 27002. Instalación y protección de equipos
4	En caso de que el mobiliario cuente con defectos. ¿Se reemplaza?	Sí.		ISO/IEC 27002. Instalación y protección de equipos
5	¿Existe un reglamento que deba seguir el personal en caso de ser nuevo en la empresa? ¿Cual?	Sí, Tener cudado con todo.		ISO/IEC 27002 Controles físicos de entrada
6	¿Existe algún tipo de formato o bitácora dónde se realicen registro del personal externo cuando hace uso de alguna maquina?	No.		ISO/IEC 27002 Controles físicos de entrada
7	¿Conoce usted si se maneja alguna norma dentro de su departamento? ¿Cuál es?	No.		ISO/IEC 27002 Controles físicos de entrada
8	¿Está usted capacitado para reaccionar en caso de emergencia?	Sí.		ISO/IEC 27002. Instalación y protección de

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 4

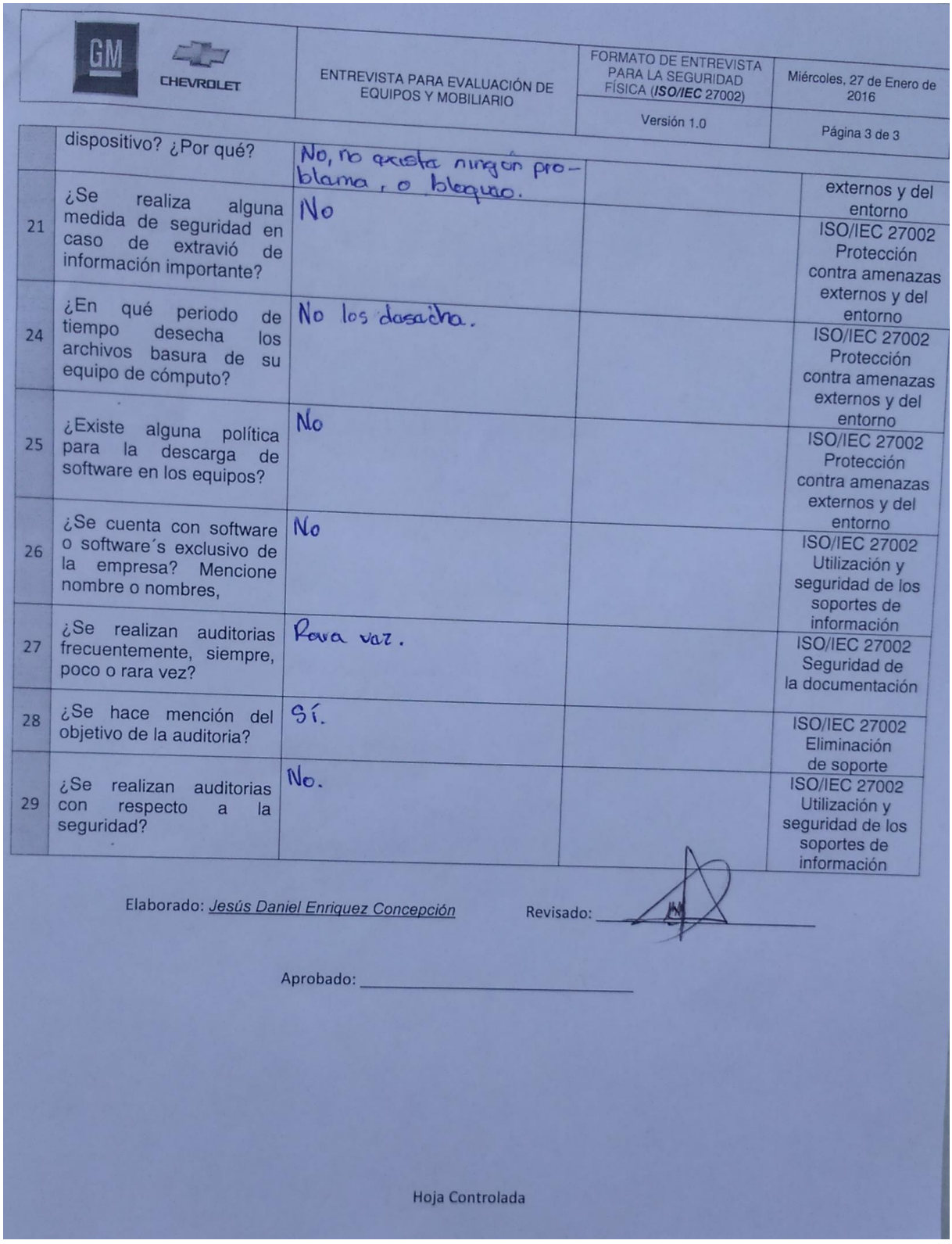


GM CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 2 de 3

				equipos
9	¿Conoce alguna norma o políticas que se manejen en la empresa en cuestión de seguridad?	Sí.		ISO/IEC 27002 Controles físicos de entrada
10	¿Se le permite a usted introducir equipos externos a la empresa (laptops)?	No.		ISO/IEC 27002. Instalación y protección de equipos
11	¿Las instalaciones cuentan con detectores de humo, en caso de incendios?	No.		ISO/IEC 27002 Protección contra amenazas
12	¿Existe algún extintor dentro de su área de trabajo? ¿Cuantos?	No.		ISO/IEC 27002 Controles físicos de entrada
13	¿En caso de fallo de algún equipo, este se sustituye?	Sí.		ISO/IEC 27002 Suministro eléctrico
14	¿Se tienen bitácoras ya sean digitales o a papel, de fallos de los equipos? Cuál es el proceso.	No		ISO/IEC 27002 Suministro eléctrico
15	¿Se realiza mantenimiento a los equipos frecuentemente?	No. exclusivamente a la copiadora.		ISO/IEC 27002 Suministro eléctrico
16	¿Se realizan respaldo de información en caso de desastres naturales?	No		ISO/IEC 27002 Protección contra amenazas externos y del entorno
17	Respalda su información frecuentemente, siempre o casi nunca.	Casi nunca		ISO/IEC 27002 Controles físicos de entrada
18	¿Se cuenta con manual de usuario sobre el uso de los equipos?	No.		ISO/IEC 27002 Controles físicos de entrada
19	¿Cada equipo de cómputo dentro de su área de trabajo cuenta con contraseña personal o es abierta para cualquier persona?	Contrasaña Parsonal.		ISO/IEC 27002 Utilización y seguridad de los soportes de información
20	¿Existe restricción para almacenar información como USB, u otro			ISO/IEC 27002 Protección contra amenazas

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 5



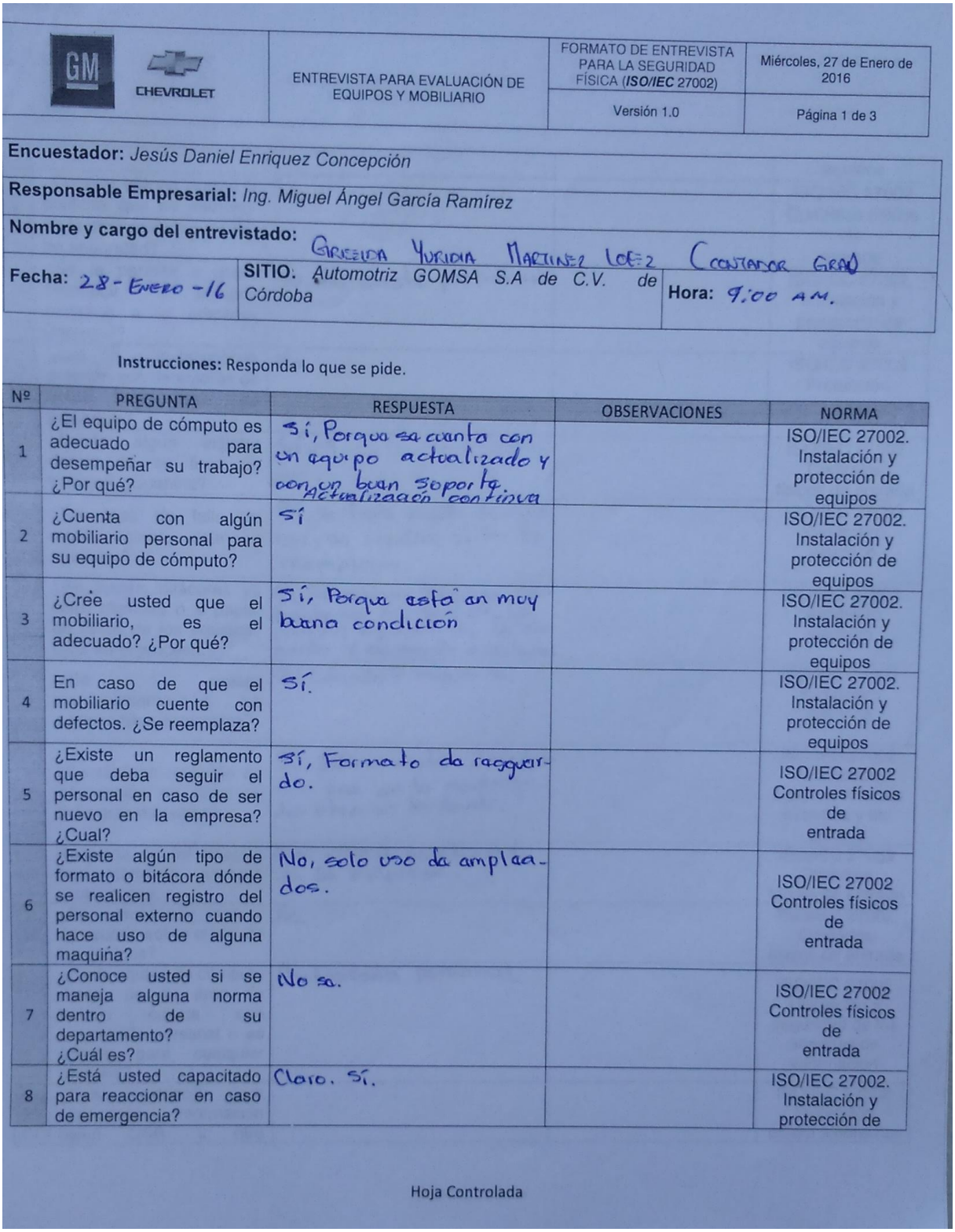
GM CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002) Versión 1.0	Miércoles, 27 de Enero de 2016 Página 3 de 3	
	dispositivo? ¿Por qué?	No, no existe ningún problema, o bloqueo.		externos y del entorno
21	¿Se realiza alguna medida de seguridad en caso de extravió de información importante?	No		ISO/IEC 27002 Protección contra amenazas externos y del entorno
24	¿En qué periodo de tiempo desecha los archivos basura de su equipo de cómputo?	No los desecha.		ISO/IEC 27002 Protección contra amenazas externos y del entorno
25	¿Existe alguna política para la descarga de software en los equipos?	No		ISO/IEC 27002 Protección contra amenazas externos y del entorno
26	¿Se cuenta con software o software´s exclusivo de la empresa? Mencione nombre o nombres,	No		ISO/IEC 27002 Utilización y seguridad de los soportes de información
27	¿Se realizan auditorias frecuentemente, siempre, poco o rara vez?	Rara vez.		ISO/IEC 27002 Seguridad de la documentación
28	¿Se hace mención del objetivo de la auditoria?	Sí.		ISO/IEC 27002 Eliminación de soporte
29	¿Se realizan auditorias con respecto a la seguridad?	No.		ISO/IEC 27002 Utilización y seguridad de los soportes de información

Elaborado: *Jesús Daniel Enriquez Concepción* Revisado: _____

Aprobado: _____

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 6



GM CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 1 de 3

Encuestador: *Jesús Daniel Enriquez Concepción*

Responsable Empresarial: *Ing. Miguel Ángel García Ramírez*

Nombre y cargo del entrevistado: Graciela Yuridia Martinez Lopez (Contador Grad)

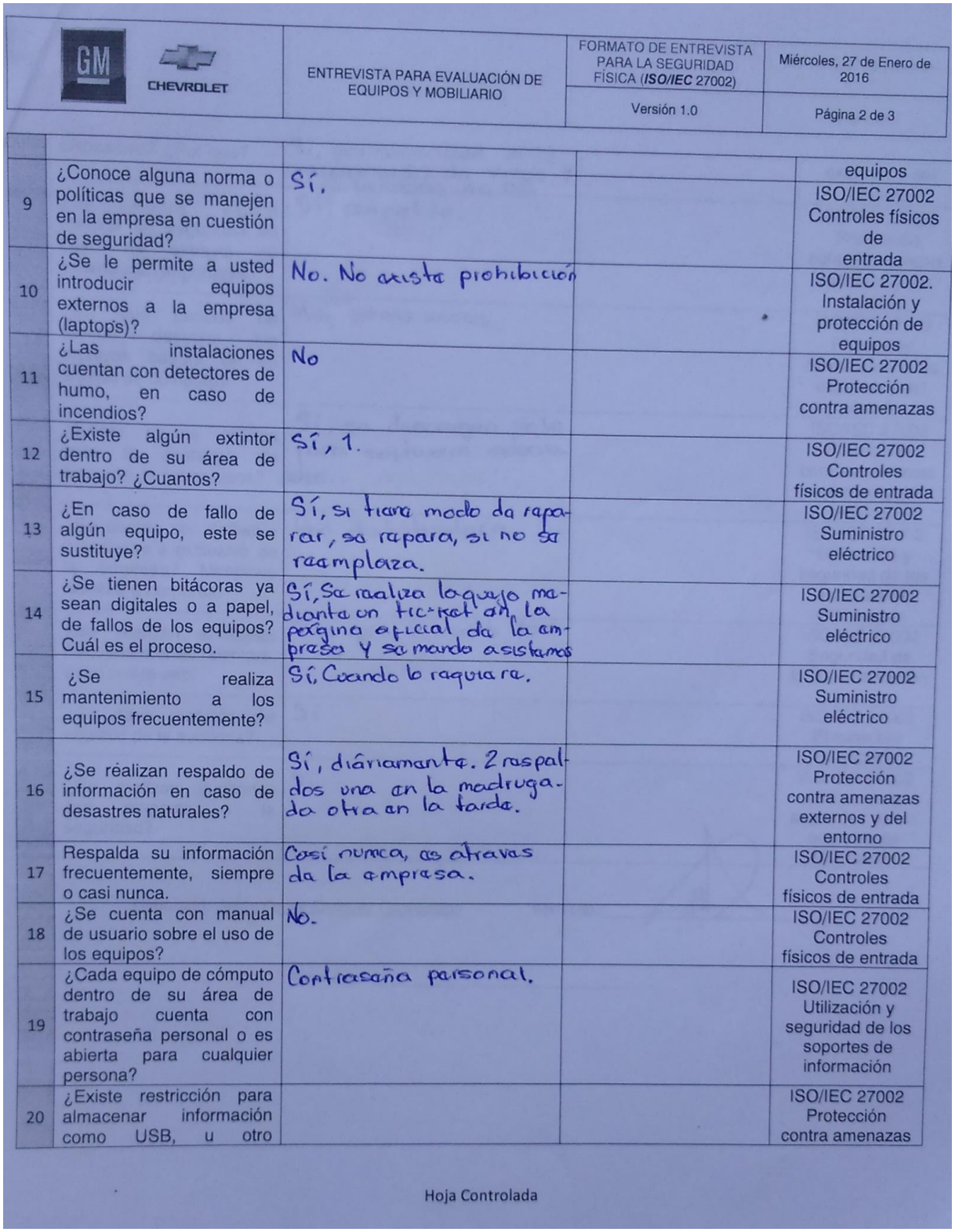
Fecha: 28-Enero-16 | **SITIO.** *Automotriz GOMSA S.A de C.V. de Córdoba* | **Hora:** 9:00 A.M.

Instrucciones: Responda lo que se pide.

Nº	PREGUNTA	RESPUESTA	OBSERVACIONES	NORMA
1	¿El equipo de cómputo es adecuado para desempeñar su trabajo? ¿Por qué?	Sí, Porque se cuenta con un equipo actualizado y con un buen soporte. Actualización continua		ISO/IEC 27002. Instalación y protección de equipos
2	¿Cuenta con algún mobiliario personal para su equipo de cómputo?	Sí		ISO/IEC 27002. Instalación y protección de equipos
3	¿Cree usted que el mobiliario, es el adecuado? ¿Por qué?	Sí, Porque están en muy buena condición		ISO/IEC 27002. Instalación y protección de equipos
4	En caso de que el mobiliario cuente con defectos. ¿Se reemplaza?	Sí.		ISO/IEC 27002. Instalación y protección de equipos
5	¿Existe un reglamento que deba seguir el personal en caso de ser nuevo en la empresa? ¿Cual?	Sí, Formato de resguardo.		ISO/IEC 27002 Controles físicos de entrada
6	¿Existe algún tipo de formato o bitácora dónde se realicen registro del personal externo cuando hace uso de alguna maquina?	No, solo uso de empleados.		ISO/IEC 27002 Controles físicos de entrada
7	¿Conoce usted si se maneja alguna norma dentro de su departamento? ¿Cuál es?	No se.		ISO/IEC 27002 Controles físicos de entrada
8	¿Está usted capacitado para reaccionar en caso de emergencia?	Claro. Sí.		ISO/IEC 27002. Instalación y protección de

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 7



GM CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 2 de 3

				equipos
9	¿Conoce alguna norma o políticas que se manejen en la empresa en cuestión de seguridad?	Sí.		ISO/IEC 27002 Controles físicos de entrada
10	¿Se le permite a usted introducir equipos externos a la empresa (laptops)?	No. No existe prohibición		ISO/IEC 27002. Instalación y protección de equipos
11	¿Las instalaciones cuentan con detectores de humo, en caso de incendios?	No		ISO/IEC 27002 Protección contra amenazas
12	¿Existe algún extintor dentro de su área de trabajo? ¿Cuantos?	Sí, 1.		ISO/IEC 27002 Controles físicos de entrada
13	¿En caso de fallo de algún equipo, este se sustituye?	Sí, si tiene modo de reparar, se repara, si no se reemplaza.		ISO/IEC 27002 Suministro eléctrico
14	¿Se tienen bitácoras ya sean digitales o a papel, de fallos de los equipos? Cuál es el proceso.	Sí, Se realiza la queja mediante un ticket en la página oficial de la empresa y se manda asistencia		ISO/IEC 27002 Suministro eléctrico
15	¿Se realiza mantenimiento a los equipos frecuentemente?	Sí, Cuando lo requiera.		ISO/IEC 27002 Suministro eléctrico
16	¿Se realizan respaldo de información en caso de desastres naturales?	Sí, diáriamente. 2 respaldos una en la madrugada otra en la tarde.		ISO/IEC 27002 Protección contra amenazas externos y del entorno
17	Respalda su información frecuentemente, siempre o casi nunca.	Casi nunca, es atravas de la empresa.		ISO/IEC 27002 Controles físicos de entrada
18	¿Se cuenta con manual de usuario sobre el uso de los equipos?	No.		ISO/IEC 27002 Controles físicos de entrada
19	¿Cada equipo de cómputo dentro de su área de trabajo cuenta con contraseña personal o es abierta para cualquier persona?	Contrasaña personal.		ISO/IEC 27002 Utilización y seguridad de los soportes de información
20	¿Existe restricción para almacenar información como USB, u otro			ISO/IEC 27002 Protección contra amenazas

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 8

GM CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 1 de 3

Encuestador: *Jesús Daniel Enriquez Concepción*

Responsable Empresarial: *Ing. Miguel Ángel García Ramírez*

Nombre y cargo del entrevistado: José Flores Victoria Advo. Posventa

Fecha: 28/01/16

SITIO: *Automotriz GOMSA S.A de C.V. de Córdoba*

Hora: 10:05 am

Instrucciones: Responda lo que se pide.

Nº	PREGUNTA	RESPUESTA	OBSERVACIONES	NORMA
1	¿El equipo de cómputo es adecuado para desempeñar su trabajo? ¿Por qué?	Si,		ISO/IEC 27002. Instalación y protección de equipos
2	¿Cuenta con algún mobiliario personal para su equipo de cómputo?	Si		ISO/IEC 27002. Instalación y protección de equipos
3	¿Cree usted que el mobiliario, es el adecuado? ¿Por qué?	No, mi silla se baja sola tuve que ponerle un soporte	/	ISO/IEC 27002. Instalación y protección de equipos
4	En caso de que el mobiliario cuente con defectos. ¿Se reemplaza?	No		ISO/IEC 27002. Instalación y protección de equipos
5	¿Existe un reglamento que deba seguir el personal en caso de ser nuevo en la empresa? ¿Cual?	Si, el reglamento interno		ISO/IEC 27002 Controles físicos de entrada
6	¿Existe algún tipo de formato o bitácora dónde se realicen registro del personal externo cuando hace uso de alguna maquina?	No ninguno. solo se registra entrada a las instalaciones		ISO/IEC 27002 Controles físicos de entrada
7	¿Conoce usted si se maneja alguna norma dentro de su departamento? ¿Cuál es?	No.		ISO/IEC 27002 Controles físicos de entrada
8	¿Está usted capacitado para reaccionar en caso de emergencia?	Si		ISO/IEC 27002. Instalación y protección de

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 9

GM CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 3 de 3

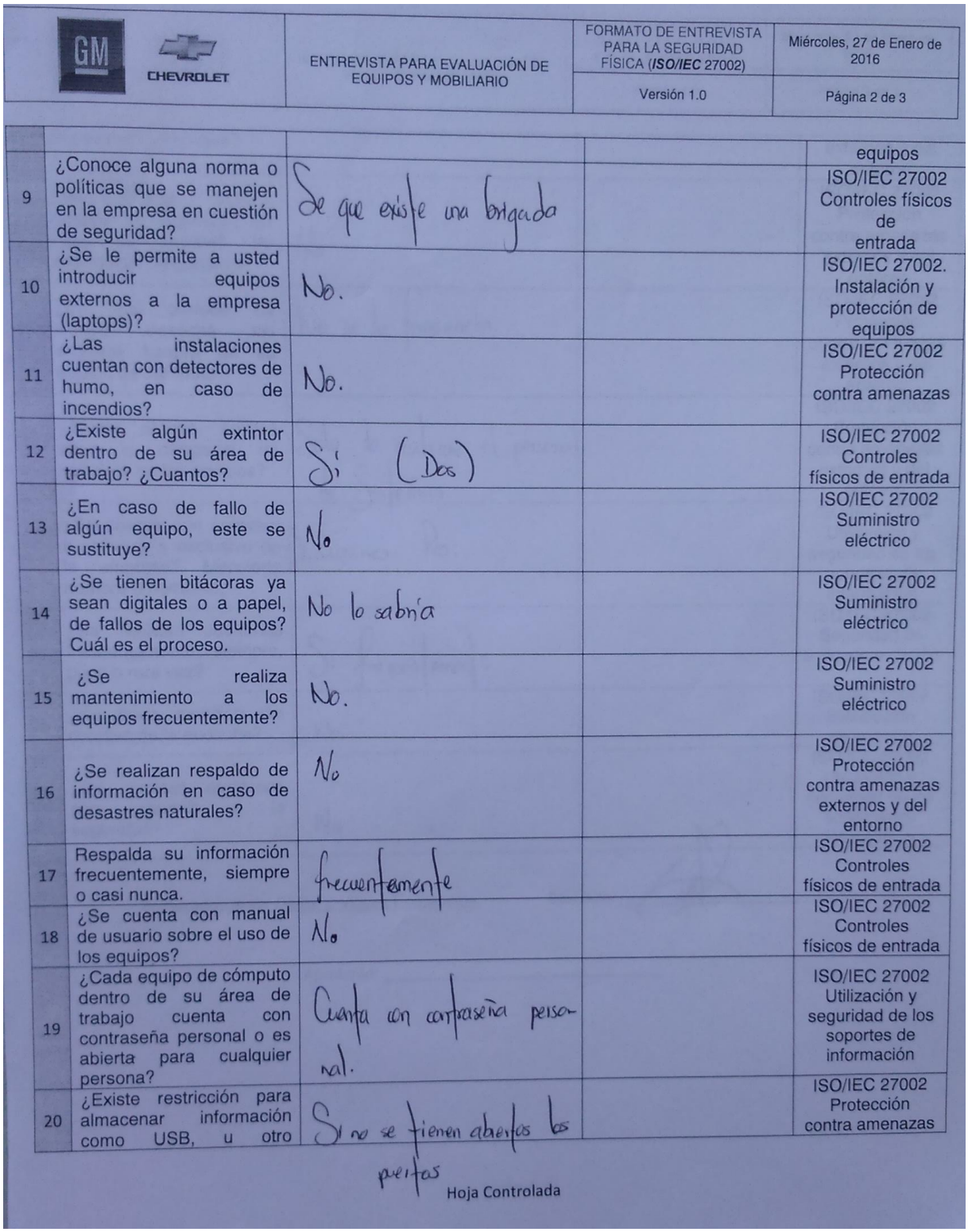
	dispositivo? ¿Por qué?	Sí, por seguridad a la información de virus. y licencias en CD.		externos y del entorno
21	¿Se realiza alguna medida de seguridad en caso de extravió de información importante?	Sí, respaldo.		ISO/IEC 27002 Protección contra amenazas externos y del entorno
24	¿En qué periodo de tiempo desecha los archivos basura de su equipo de cómputo?	Muy pocas vacas.		ISO/IEC 27002 Protección contra amenazas externos y del entorno
25	¿Existe alguna política para la descarga de software en los equipos?	Sí, se descargan solo para software ordenados.		ISO/IEC 27002 Protección contra amenazas externos y del entorno
26	¿Se cuenta con software o software´s exclusivo de la empresa? Mencione nombre o nombres,	Red distribuidora.		ISO/IEC 27002 Utilización y seguridad de los soportes de información
27	¿Se realizan auditorias frecuentemente, siempre, poco o rara vez?	Siempre, 2 veces por año		ISO/IEC 27002 Seguridad de la documentación
28	¿Se hace mención del objetivo de la auditoria?	Sí		ISO/IEC 27002 Eliminación de soporte
29	¿Se realizan auditorias con respecto a la seguridad?	Sí.		ISO/IEC 27002 Utilización y seguridad de los soportes de información

Elaborado: *Jesús Daniel Enriquez Concepción* Revisado: _____

Aprobado: _____

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 10

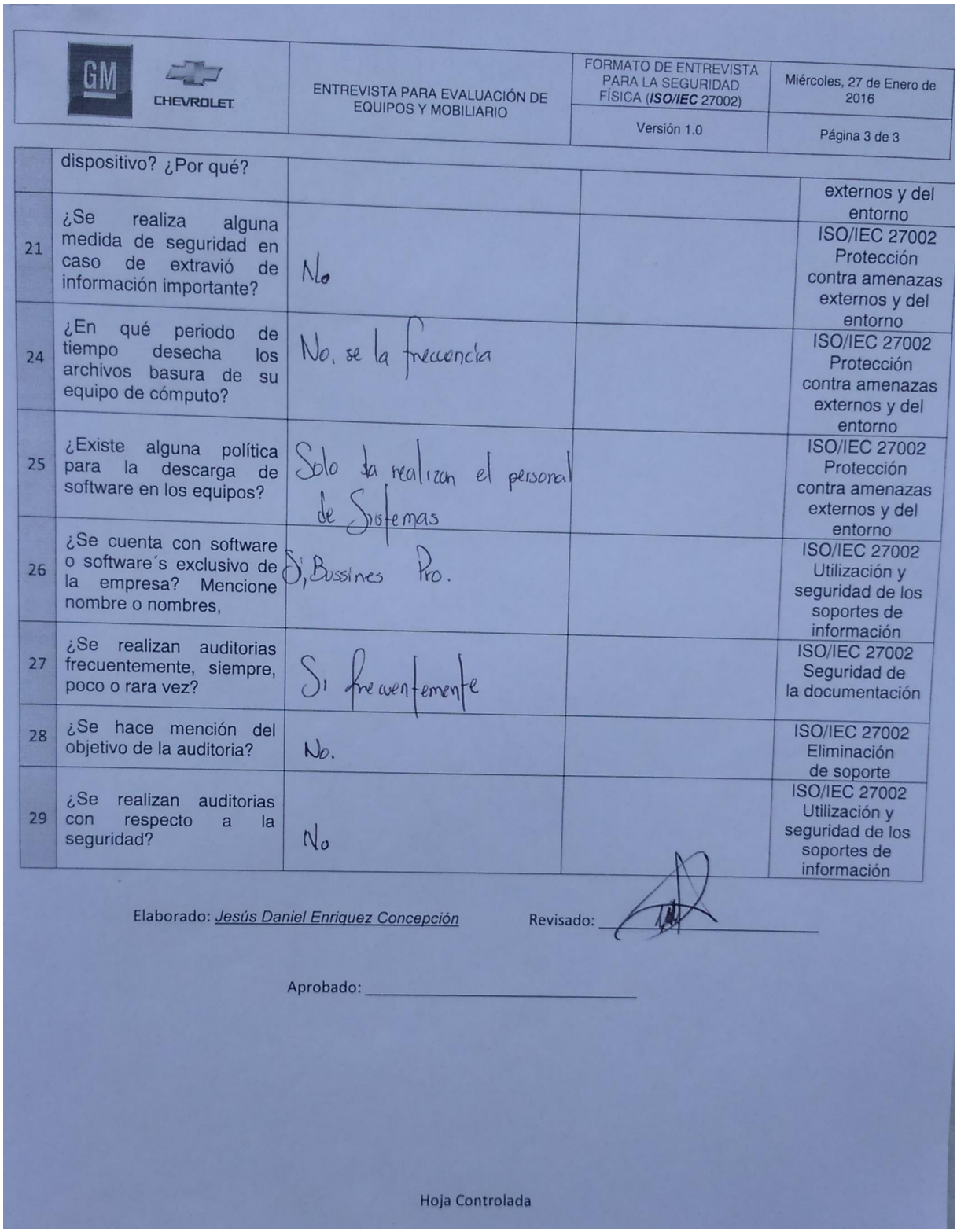


GM CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 2 de 3

				equipos
9	¿Conoce alguna norma o políticas que se manejen en la empresa en cuestión de seguridad?	Se que existe una brigada		ISO/IEC 27002 Controles físicos de entrada
10	¿Se le permite a usted introducir equipos externos a la empresa (laptops)?	No.		ISO/IEC 27002. Instalación y protección de equipos
11	¿Las instalaciones cuentan con detectores de humo, en caso de incendios?	No.		ISO/IEC 27002 Protección contra amenazas
12	¿Existe algún extintor dentro de su área de trabajo? ¿Cuantos?	Si (Dos)		ISO/IEC 27002 Controles físicos de entrada
13	¿En caso de fallo de algún equipo, este se sustituye?	No		ISO/IEC 27002 Suministro eléctrico
14	¿Se tienen bitácoras ya sean digitales o a papel, de fallos de los equipos? Cuál es el proceso.	No lo sabría		ISO/IEC 27002 Suministro eléctrico
15	¿Se realiza mantenimiento a los equipos frecuentemente?	No.		ISO/IEC 27002 Suministro eléctrico
16	¿Se realizan respaldo de información en caso de desastres naturales?	No		ISO/IEC 27002 Protección contra amenazas externos y del entorno
17	Respalda su información frecuentemente, siempre o casi nunca.	frecuentemente		ISO/IEC 27002 Controles físicos de entrada
18	¿Se cuenta con manual de usuario sobre el uso de los equipos?	No		ISO/IEC 27002 Controles físicos de entrada
19	¿Cada equipo de cómputo dentro de su área de trabajo cuenta con contraseña personal o es abierta para cualquier persona?	Cuenta con contraseña personal.		ISO/IEC 27002 Utilización y seguridad de los soportes de información
20	¿Existe restricción para almacenar información como USB, u otro	Si no se tienen abiertos los puertos		ISO/IEC 27002 Protección contra amenazas

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 11



GM CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 3 de 3

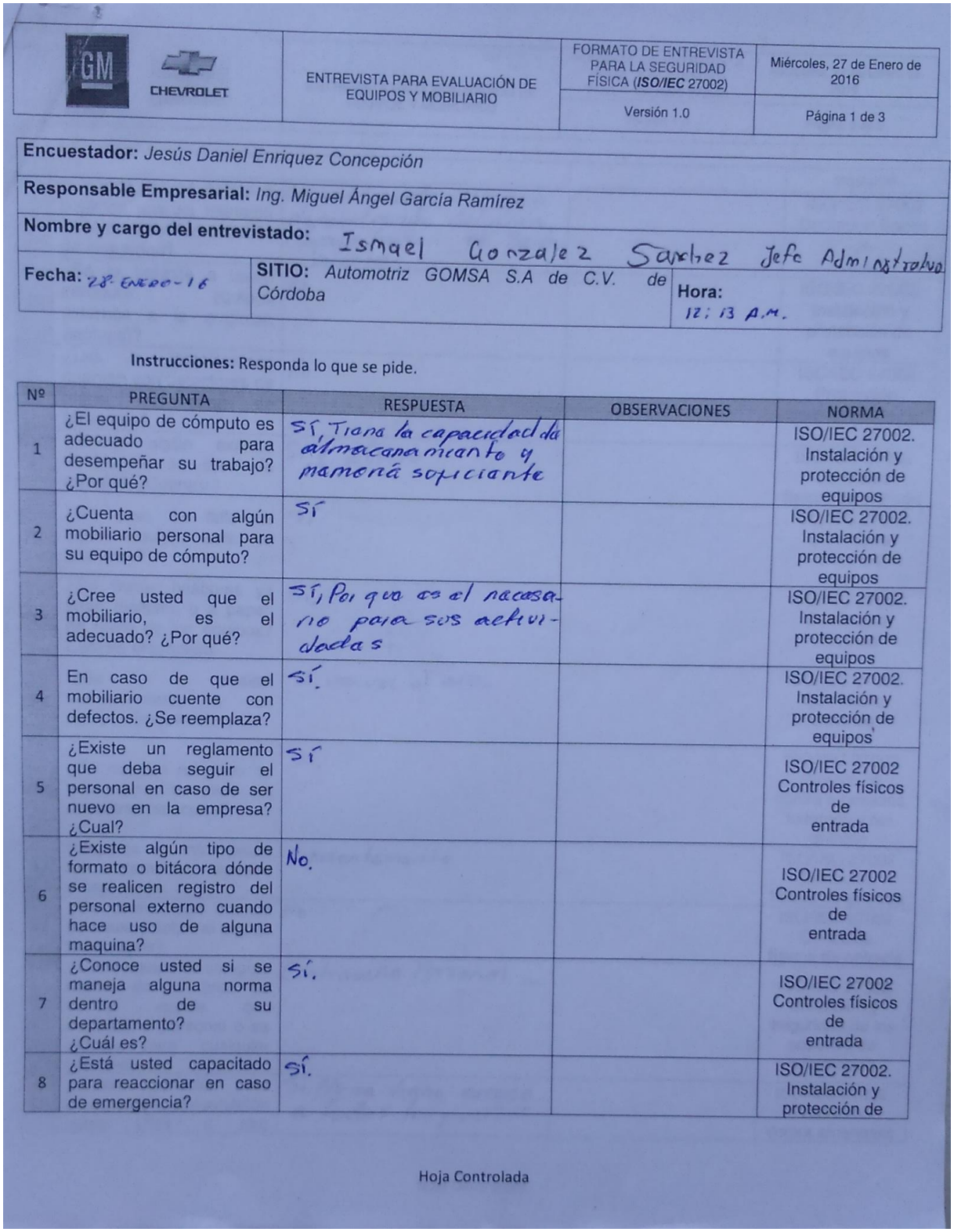
	dispositivo? ¿Por qué?			externos y del entorno
21	¿Se realiza alguna medida de seguridad en caso de extravió de información importante?	No		ISO/IEC 27002 Protección contra amenazas externos y del entorno
24	¿En qué periodo de tiempo desecha los archivos basura de su equipo de cómputo?	No, se la frecuencia		ISO/IEC 27002 Protección contra amenazas externos y del entorno
25	¿Existe alguna política para la descarga de software en los equipos?	Solo la realizan el personal de Sistemas		ISO/IEC 27002 Protección contra amenazas externos y del entorno
26	¿Se cuenta con software o software´s exclusivo de la empresa? Mencione nombre o nombres,	Sí, Bussines Pro.		ISO/IEC 27002 Utilización y seguridad de los soportes de información
27	¿Se realizan auditorias frecuentemente, siempre, poco o rara vez?	Sí frecuentemente		ISO/IEC 27002 Seguridad de la documentación
28	¿Se hace mención del objetivo de la auditoria?	No.		ISO/IEC 27002 Eliminación de soporte
29	¿Se realizan auditorias con respecto a la seguridad?	No		ISO/IEC 27002 Utilización y seguridad de los soportes de información

Elaborado: *Jesús Daniel Enriquez Concepción* Revisado: _____

Aprobado: _____

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 12



	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 1 de 3

Encuestador: *Jesús Daniel Enriquez Concepción*

Responsable Empresarial: *Ing. Miguel Ángel García Ramírez*

Nombre y cargo del entrevistado: Ismael Gonzalez Sanchez Jefe Administrativo

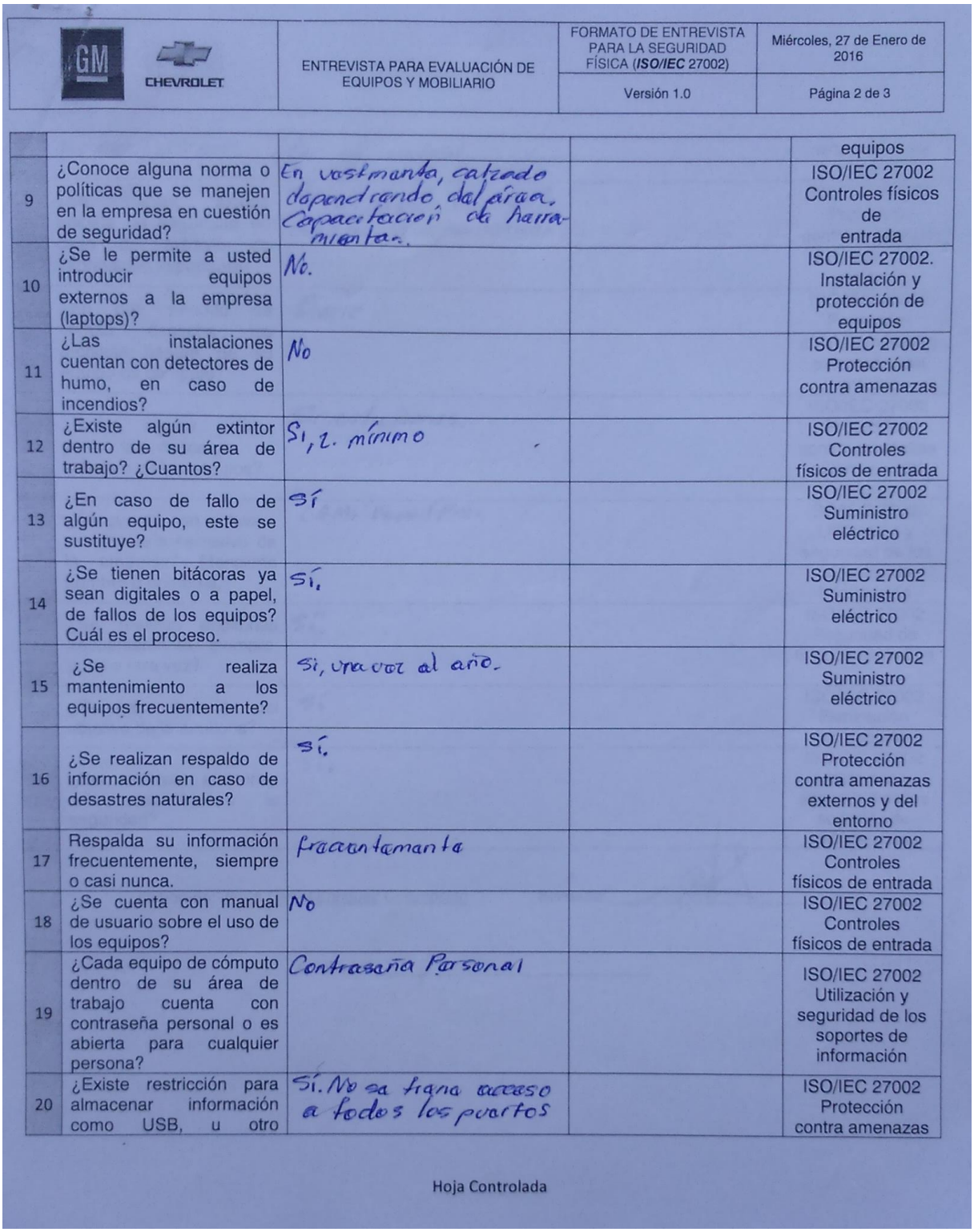
Fecha: 28 ENERO-16 | **SITIO:** *Automotriz GOMSA S.A de C.V. de Córdoba* | **Hora:** 12:13 A.M.

Instrucciones: Responda lo que se pide.

Nº	PREGUNTA	RESPUESTA	OBSERVACIONES	NORMA
1	¿El equipo de cómputo es adecuado para desempeñar su trabajo? ¿Por qué?	Sí, Tiene la capacidad de almacenamiento y memoria suficiente		ISO/IEC 27002. Instalación y protección de equipos
2	¿Cuenta con algún mobiliario personal para su equipo de cómputo?	Sí		ISO/IEC 27002. Instalación y protección de equipos
3	¿Cree usted que el mobiliario, es el adecuado? ¿Por qué?	Sí, Por que es el necesario para sus actividades		ISO/IEC 27002. Instalación y protección de equipos
4	En caso de que el mobiliario cuente con defectos. ¿Se reemplaza?	Sí.		ISO/IEC 27002. Instalación y protección de equipos
5	¿Existe un reglamento que deba seguir el personal en caso de ser nuevo en la empresa? ¿Cual?	Sí		ISO/IEC 27002 Controles físicos de entrada
6	¿Existe algún tipo de formato o bitácora dónde se realicen registro del personal externo cuando hace uso de alguna maquina?	No.		ISO/IEC 27002 Controles físicos de entrada
7	¿Conoce usted si se maneja alguna norma dentro de su departamento? ¿Cuál es?	Sí.		ISO/IEC 27002 Controles físicos de entrada
8	¿Está usted capacitado para reaccionar en caso de emergencia?	Sí.		ISO/IEC 27002. Instalación y protección de

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 13

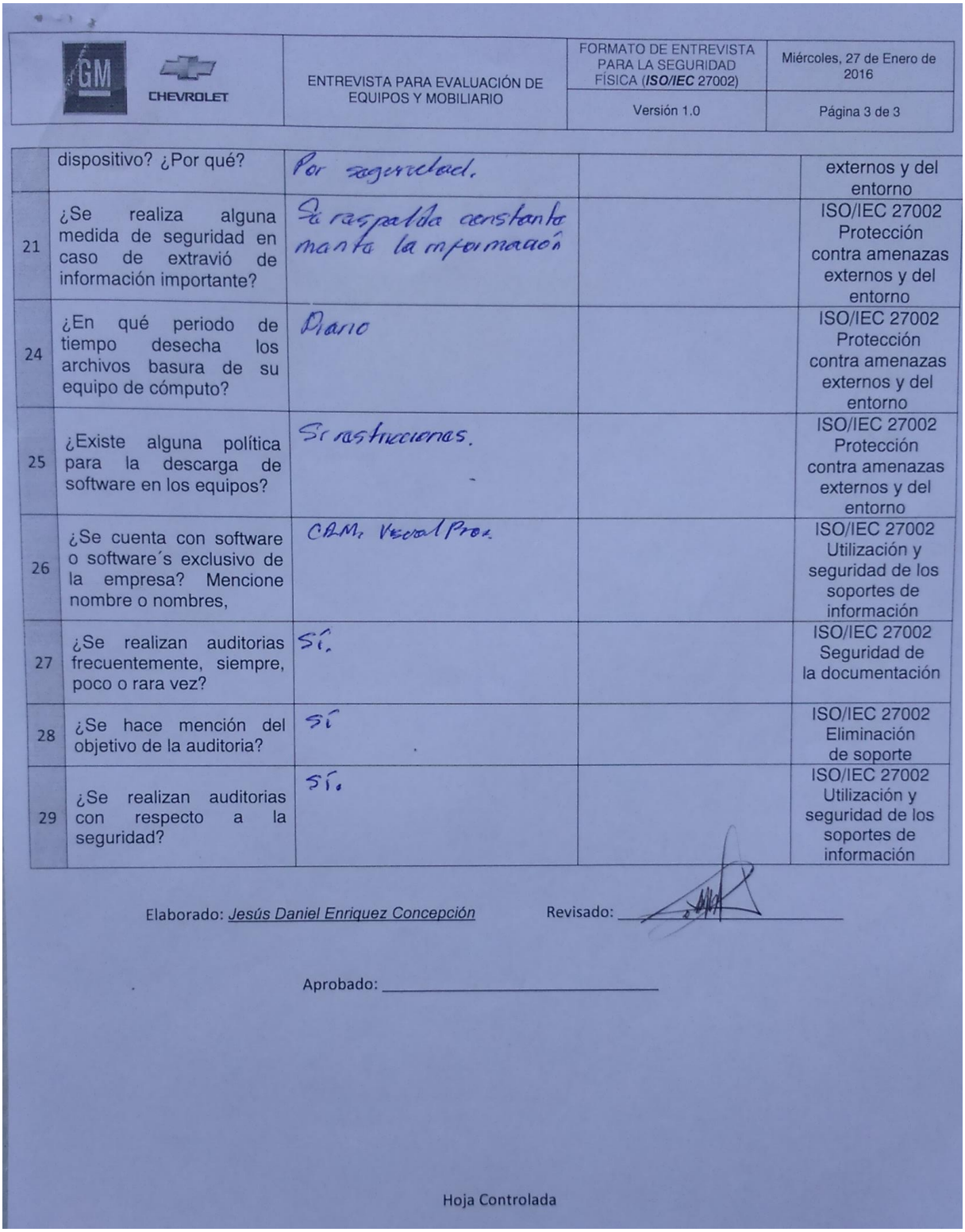


GM CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 2 de 3

				equipos
9	¿Conoce alguna norma o políticas que se manejen en la empresa en cuestión de seguridad?	En vestimenta, calzado dependiendo del área, Capacitación de herramienta.		ISO/IEC 27002 Controles físicos de entrada
10	¿Se le permite a usted introducir equipos externos a la empresa (laptops)?	No.		ISO/IEC 27002. Instalación y protección de equipos
11	¿Las instalaciones cuentan con detectores de humo, en caso de incendios?	No		ISO/IEC 27002 Protección contra amenazas
12	¿Existe algún extintor dentro de su área de trabajo? ¿Cuantos?	Si, 2. mínimo		ISO/IEC 27002 Controles físicos de entrada
13	¿En caso de fallo de algún equipo, este se sustituye?	Sí		ISO/IEC 27002 Suministro eléctrico
14	¿Se tienen bitácoras ya sean digitales o a papel, de fallos de los equipos? Cuál es el proceso.	Sí.		ISO/IEC 27002 Suministro eléctrico
15	¿Se realiza mantenimiento a los equipos frecuentemente?	Si, una vez al año.		ISO/IEC 27002 Suministro eléctrico
16	¿Se realizan respaldo de información en caso de desastres naturales?	Sí.		ISO/IEC 27002 Protección contra amenazas externos y del entorno
17	Respalda su información frecuentemente, siempre o casi nunca.	Frecuentemente		ISO/IEC 27002 Controles físicos de entrada
18	¿Se cuenta con manual de usuario sobre el uso de los equipos?	No		ISO/IEC 27002 Controles físicos de entrada
19	¿Cada equipo de cómputo dentro de su área de trabajo cuenta con contraseña personal o es abierta para cualquier persona?	Contraseña Personal		ISO/IEC 27002 Utilización y seguridad de los soportes de información
20	¿Existe restricción para almacenar información como USB, u otro	Sí. No se tiene acceso a todos los puertos		ISO/IEC 27002 Protección contra amenazas

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 14



GM CHEVROLET	ENTREVISTA PARA EVALUACIÓN DE EQUIPOS Y MOBILIARIO	FORMATO DE ENTREVISTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 3 de 3

	dispositivo? ¿Por qué?	Por seguridad.		externos y del entorno
21	¿Se realiza alguna medida de seguridad en caso de extravió de información importante?	Se respalda constante manta la información		ISO/IEC 27002 Protección contra amenazas externos y del entorno
24	¿En qué periodo de tiempo desecha los archivos basura de su equipo de cómputo?	Diario		ISO/IEC 27002 Protección contra amenazas externos y del entorno
25	¿Existe alguna política para la descarga de software en los equipos?	Si restricciones.		ISO/IEC 27002 Protección contra amenazas externos y del entorno
26	¿Se cuenta con software o software´s exclusivo de la empresa? Mencione nombre o nombres,	CAM, Vecral Pro.		ISO/IEC 27002 Utilización y seguridad de los soportes de información
27	¿Se realizan auditorias frecuentemente, siempre, poco o rara vez?	Sí.		ISO/IEC 27002 Seguridad de la documentación
28	¿Se hace mención del objetivo de la auditoria?	Sí		ISO/IEC 27002 Eliminación de soporte
29	¿Se realizan auditorias con respecto a la seguridad?	Sí.		ISO/IEC 27002 Utilización y seguridad de los soportes de información

Elaborado: *Jesús Daniel Enriquez Concepción* Revisado: _____

Aprobado: _____

Hoja Controlada

Evidencia_Formato_Entrevista 1.1 15

GM CHEVROLET	ENCUESTA	FORMATO DE ENCUESTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 1 de 2

Encuestador: *Jesús Daniel Enriquez Concepción*		
Responsable Empresarial: *Ing. Miguel Ángel García Ramírez*		
Nombre y cargo del encuestado: Soporte de Sistemas		
Fecha: 28/01/16	**SITIO:** *Automotriz GOMSA S.A de C.V. de Córdoba*	**Hora:** 9:00

Instrucciones: Marque con una x según corresponda su respuesta.

Nº	PREGUNTA	CUMPLE		OBSERVACIONES
		SI	NO	
1	¿La ubicación del centro de cómputo está seguro de inundaciones, robo o cualquier otra situación que pueda poner en peligro los equipos?	/		
2	¿En el área de cómputo se cuentan con armarios ignífugos (anti fuegos)?		/	
3	¿Dentro del área existen materiales que sean inflamables, o puedan causar algún daño a los equipos?		/	
4	¿Existe espacio suficiente para los equipos?	/		
5	¿Es adecuada la iluminación dentro del área?	/		
6	¿La temperatura en la que trabajan los equipos es la adecuada para su durabilidad?	/		
7	¿Dentro del área de cómputo, existen equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, UPS, generadores de energía?	/		
8	¿Existe procedimiento de mantenimiento por parte de la empresa, en el centro de cómputo?	/		
9	¿Existe una sala o edificio donde se encuentre alojado el servidor?	/		
10	¿Los cables están bien instalados dentro del centro de cómputo, es decir si se encuentran dentro de canales o paneles?	/		
11	¿Los equipos cuentan con antivirus?	/		
12	¿Se lleva un registro de incidencias de virus en cada equipo?	/		
13	¿El cableado de red de los equipos se encuentra etiquetado?	/		
14	¿Se cuenta con un sistema puesta a tierra para los equipos de cómputo en caso de descargas eléctricas?	/		
15	¿Los antivirus instalados son adecuados para la eliminación de virus en los equipos?	/		
16	¿Existen políticas para la seguridad de la información en los equipos de cómputo de cada departamento?	/		
17	¿Dichas políticas están documentadas?	/		
18	¿El acceso a los equipos del centro de cómputo, cuentan con medidas de seguridad para acceder a ellos?	/		

Hoja Controlada

Evidencia_Formato_Encuesta 1.1 1

GM CHEVROLET	ENCUESTA	FORMATO DE ENCUESTA PARA LA SEGURIDAD FÍSICA (*ISO/IEC* 27002)	Miércoles, 27 de Enero de 2016
		Versión 1.0	Página 2 de 2

19	¿Se tienen implementadas dichas contraseñas en cada equipo?	✓		
20	¿Se emplean cuentas de usuario para cada terminal en cada departamento?	✓		
21	¿Cuentan con inventario o inventarios de los equipos de cómputo?	✓		
22	¿Se realiza un chequeo frecuente del inventario de los equipos?	✓		
23	¿Se cuenta con instalación eléctrica específicamente para los equipos de cómputo?	✓		
24	¿Se tienen bitácoras para el acceso del personal a los equipos de cómputo?	✓		
25	¿Los equipos de cómputos se encuentran conectados a UPS o algún tipo de regulador eléctrico?	✓		
26	¿Existen normas o políticas para el acceso del personal externo a la empresa?	✓		
27	¿Dichas normas o políticas se tienen documentadas?	✓		
28	¿Cuentan con extintores, sistema contra incendios donde se encuentran los equipos?	✓		
29	¿Cuentan con alguna topología de red?	✓		Estrella
30	¿En caso de que el nuevo personal de la empresa acceda al centro de cómputo, se le facilita usando los manuales (Técnico – Usuario si se cuenta)?	✓		
31	¿La información de los equipos se encuentra a salvo de terremotos, inundaciones, incendios o algún otro tipo de desastre natural?	✓		

Elaborado: *Jesús Daniel Enriquez Concepción* Revisado: _____

Aprobado: _____

Hoja Controlada

Evidencia_Formato_Encuesta 1.1 2