ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN DE MITIGACIÓN DE MALWARE, INGENIERÍA SOCIAL Y VIOLACIÓN DE CONTRASEÑAS PARA UNA ORGANIZACIÓN NO GUBERNAMENTAL INTERNACIONAL BASADA EN ISO/IEC27001:2013"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

CHRISTIAN ALEJANDRO RIVADENEIRA ZAMORA

Guayaquil – Ecuador

2016

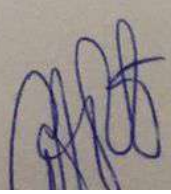
AGRADECIMIENTO

Todo lo que hacemos debe ser el resultado de nuestra gratitud por lo que Dios ha hecho por nosotros.

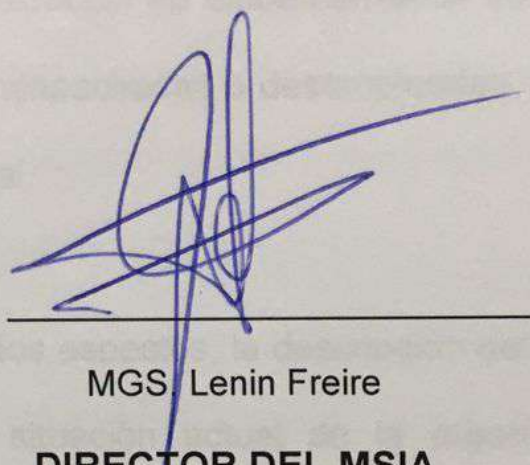
-William Arthur Ward.

DEDICATORIA

El presente trabajo está dedicado de manera especial a tres inigualables amigos: Denisse Cayetano (@_denk) y Diego Lavayen (@iakomus) quienes me impulsaron a tomar la maestría, y Margarita Filian (@wiwiwii) quien con paciencia y conocimiento supo aclararme las millones de dudas existenciales generadas durante varias materias; adicionalmente, y no menos importante, está dedicada a MBA. Jenny Virginia Duarte Tapia, todos mis irremplazables amigos y a mis queridos familiares, quienes me aportaron con su grano de arena para cumplir un objetivo más en esta aventura llamada vida. ¡Gracias!

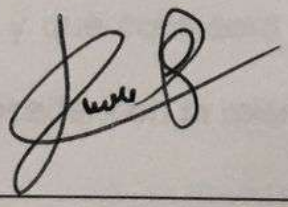


TRIBUNAL DE SUSTENTACIÓN



MGS. Lenin Freire

DIRECTOR DEL MSIA



MGS. Juan Carlos García

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA

RESUMEN

El presente trabajo muestra una auditoría, basada en la norma ISO/IEC 27001:2013, a una Organización no Gubernamental que está orientada a la asistencia de personas incapacitadas o desempleadas, servicios de caridad, y rehabilitación profesional.

El Capítulo 1 considera dos aspectos, la descripción del problema, el cual se enfoca en describir la situación actual de la organización reflejada en reportes que se reciben como parte de la medición de resultados, y la debilidad de la misma ante una escasa cultura de seguridad de información en todos los niveles del organigrama; el segundo aspecto destaca la solución propuesta, la misma que propone obtener un estado de la organización mediante una auditoría enfocada, y que considera a la ISO/IEC 27001:2013 como un referente idóneo para proceder con la misma.

El Capítulo 2 detalla la metodología de desarrollo de la solución, es el capítulo más extenso y en el que se describe la planificación de la auditoría, la cual se inicia con el levantamiento de información de, ¿quién es el cliente? Llegar a la definición de los objetivos y el alcance de los mismos, son los puntos esenciales para poder proceder con la revisión documental y preparar la auditoría en sitio.

El Capítulo 3 comprende el análisis de resultados, es el capítulo más importante porque revela el estado de la organización a través de los resultados de la auditoría. Como parte de éste capítulo, se considera la sección de plan de resolución de no conformidades u observaciones; bajo el cual se expresa los acuerdos a los que el cliente llegó para crear, modificar y mejorar todas aquellas no conformidades encontradas e implementar todas aquellas recomendaciones aceptadas.

La última sección muestra las conclusiones y recomendaciones a las que se llegaron al culminar el presente trabajo de auditoría.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

BBB	*Better Business Bureau*
EEUU	Estados Unidos
IEC	*International Electro technical Commission*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
MDB	Archivo de Base de Datos utilizado por *Microsoft Office*
ONG	Organización no Gubernamental
POP3	*Post Office Protocol 3*
SGSI	Sistema de Gestión de la Seguridad de la Información

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Teniendo en cuenta que hoy en día el entorno tecnológico es extremadamente cambiante y dinámico, son muchos los nuevos escenarios que pueden presentarse y que nos pueden representar una amenaza [2].

Toda persona responsable de una organización siempre quiere conocer cómo se encuentra la misma, y en ocasiones se opta por evaluar la organización en relación a un referente certificado; todo esto con el único fin de mejorar, de poder aplicar los correctivos necesarios en caso de que se identifiquen procesos que necesiten un poco más de atención.

Evaluar una organización a través de una auditoría global o enfocada es una buena práctica de conocer el estado de la misma; la ISO/IEC 27001:2013 es una norma internacional [3] que describe, sin importar la naturaleza de la organización, cómo gestionar la seguridad de la información; y es bajo esta norma que se decidió realizar la auditoría con el fin de identificar posibles vulnerabilidades que, bajo la cultura actual de Seguridad de la Información, no están ayudando a mitigar la presencia de malware en los computadores, y a evitar ser víctimas

tanto de la ingeniería social como de la violación de contraseñas.

CAPÍTULO 1

GENERALIDADES

1.1. Descripción del problema

Indistintamente del lugar bajo el cual se realiza una auditoría, hay un problema que se encuentra presente en la mayoría de instituciones públicas y privadas, y es la falta de prudencia por parte de los propios empleados al manipular medios extraíbles y compartir información.

Se pueden adoptar distintos mecanismos de defensa para proteger lo más valioso que tiene la ONG, la información; sin embargo, todos ellos resultarán inútiles si el capital humano no se encuentra debidamente capacitado y con el criterio acertado para actuar bajo las actividades que se realizan de manera diaria.

Como un medio de control a nivel regional, se nos envía de manera mensual algunos reportes que ayudan a monitorear el estado de la ONG bajo tres aspectos:

- En el campo de las detecciones de malware, se puede revisar los nombres de equipo que han identificado la presencia de código malicioso, así como también el registro caducado de la versión de la base de datos del aplicativo antivirus.
- Conexiones no confiables, entre equipos servidores no autorizados y los equipos computacionales de la red local.
- De actualizaciones pendientes, para equipos servidores y equipos administrativos que tienen pendientes la instalación de actualizaciones Microsoft de nivel crítico.

Bajo el actual esquema se ha podido apagar incendios. Cada reporte nos revela una imagen de la situación de la ONG en un instante de tiempo; sin embargo, es necesario establecer una cultura de seguridad de información en todos los niveles, de tal forma que no sólo podamos mitigar presencia de malware en nuestros equipos, sino que contemos con un ambiente bajo el cual podamos trabajar y actuar de manera correcta bajo posibles nuevas amenazas.

Adicionalmente, hay que recalcar el hecho de que la mayoría de los empleados no mantiene un recelo con la información que se encuentra bajo su responsabilidad y con la que puede ser compartida. Hemos realizado una encuesta corta al personal interno y los resultados obtenidos nos han revelado inclusive las claves de acceso de sus computadores.

En un pequeño ejercicio interno, se realizó una llamada externa de “urgencia” por parte de un proveedor ficticio al departamento de compras, en el cual se especificaba que la cotización previamente solicitada ya se había enviado al correo electrónico. El “problema” se presentaba porque dicho correo “nunca llegaba” a la bandeja de entrada de la asistente de compra, para lo cual el proveedor ficticio

ofreció ayudarla, obteniendo así la dirección del servidor de correo POP3 y el usuario de conexión.

Debido a todo lo anteriormente expuesto es necesario una auditoría interna exhaustiva para así poder identificar qué procedimientos y reglas no se están gestionando de una manera adecuada, con el fin de recomendar las acciones pertinentes para mitigar el malware, la ingeniería social y la violación de contraseñas.

1.2. Solución propuesta

Toda medida de seguridad es poca en la actualidad; sin embargo, de nuestra parte se encuentra tratar de minimizar las formas en las que podemos ser víctimas de algún tipo de ataque y perdamos parte o todo del activo más valiosos, la información.

La ISO/IEC 27001:2013 es una norma internacional que describe cómo gestionar la seguridad de la información en una organización indistintamente del tipo [3] y de su naturaleza; y es bajo esta norma que se decidió realizar la auditoría con el fin de identificar posibles vulnerabilidades que, bajo la cultura actual de Seguridad de la Información, no están ayudando a mitigar la presencia de malware en nuestros computadores, y a evitar ser víctimas tanto de la ingeniería

social como de la violación de contraseñas.

La auditoría planteada nos ayudará a identificar cómo dentro de la ONG se llevan a cabo las prácticas de Seguridad de la Información mediante el esquema actual, el cual nos ayuda a gestionar la información, con el fin de mantenerla segura, en teoría. Una mala administración de la información puede resultar en serios daños a la reputación de la ONG y al día a día de las operaciones.

La auditoría propuesta pretende englobar y determinar los siguientes puntos de ejecución:

1. Ejecutar una estrategia de auditoría de seguridad informática basada en el riesgo en cumplimiento con las normas de auditoría, asegurando que todas las áreas de riesgo clave sean auditadas.
2. Plan de auditoría específica para determinar si la información está protegida, controlada y proporciona valor a la organización.
3. Llevar a cabo la auditoría de acuerdo con la ISO/IEC 27001:2013 para alcanzar los objetivos de auditoría planeados.
4. Comunicar los resultados de auditoría y hacer

recomendaciones a las partes interesadas clave a través de reuniones e informes de auditoría para promover el cambio cuando sea necesario.

5. Llevar a cabo auditorías de seguimiento para determinar si las acciones apropiadas han sido tomadas por la administración en el momento oportuno.

Con el resultado de la auditoría se espera recomendar de manera efectiva y asertiva la mejora continua de los procesos comprometidos, identificados y detallados en el título del presente documento.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1. Planeación de la auditoría

Cliente**:** Organización no gubernamental cuya actividad económica principal es la asistencia para personas incapacitadas o desempleadas, servicios de caridad, y rehabilitación profesional.

Acerca del cliente: La ONG es una fundación que ayuda a niños y familias que viven en extrema pobreza en varios países (Colombia, República Dominicana, Ecuador, Guatemala, Honduras, India, Kenia, México, Filipinas, Estados Unidos, y Zambia).

En Ecuador mantiene oficinas en las ciudades de Quito y Guayaquil, siendo la última la que mayor número de apadrinados mantiene. Cada agencia se compone de una Oficina Central y Centros Comunitarios. En el caso de la agencia que opera en Guayaquil, se tiene una Oficina Central y seis Centros Comunitarios.

Los centros comunitarios están ubicados estratégicamente en las zonas marginales del norte de la ciudad de Guayaquil, proporcionando recursos, programas y servicios que les permiten disminuir el peso de la pobreza a los niños y jóvenes de escasos recursos registrados en el programa de apadrinamiento, invirtiendo en su potencial y dándoles oportunidades para que crezcan sanos, educados y preparados para salir adelante en la sociedad y contribuir a la misma.

La ONG es una entidad benéfica acreditada por *Better Business Bureau* (BBB) y poseedor del sello del *Wise Giving Alliance*. Para poseer este sello, las entidades deben pasar una evaluación rigurosa hecha por BBB *Wise Giving Alliance* (el organismo evaluador de entidades benéficas de mayor experiencia en EEUU) y satisfacer los 20 estándares para el comportamiento responsable en las entidades benéficas —estándares que sobrepasan los que son requeridos por los reguladores gubernamentales. El sello es un símbolo que

comunica a los donantes que la organización portadora de dicho sello está comprometida a la responsabilidad y a las prácticas éticas.

Carta de Aceptación: Luego de un diálogo formal y presencial, se nos informó formalmente que: *La Dirección de la organización ha autorizado, por primera vez, la auditoría de las prácticas informáticas de la ONG. La auditoría se iniciará inmediatamente y se llevará a cabo en nombre de la ONG por Christian Alejandro Rivadeneira Zamora.*

Para su conocimiento, esta auditoría fue impulsada por algunas novedades reportadas en el último trimestre en cuanto a desvíos sensibles de los promedios conseguidos habitualmente, y ciertos síntomas de inseguridad graves que se observaron durante un muestreo con cuestionarios que se realizaron durante el último mes en varios puntos y sectores administrativos y de campo. Debido al resultado de estas encuestas, la Dirección decidió que se justificaba una auditoría inicial inmediata de las prácticas y procedimientos con respecto a los siguientes puntos: Mitigación de Malware, Ingeniería Social y violación de contraseñas.

La auditoría se llevará a cabo de plena conformidad con la política interna, identificada como Manual de Campo, bajo el estándar ISO270001:2013, y con el apoyo del Gerente de Tecnologías de Información, el Auditor Contable Interno y Dirección. Entre otras cosas, que la política establece que "...todas las actividades informáticas pendientes presentadas por la ONG objeto de la auditoría quedarán en suspenso hasta que se conozcan los resultados de la auditoría". Asimismo, de conformidad con la política, "...en función de los resultados de la auditoría, quedará a discreción exclusiva del Comité de Auditoría Informática para determinar cuándo, y en qué grado, se implementarán las recomendaciones recibidas".

Esperamos ser de su completa cooperación para que la auditoría pueda llevarse a cabo de forma rápida y llegue a la conclusión tan pronto como sea posible.

Objetivos:

- Verificar la eficiencia de las operaciones en las áreas funcionales.
- Verificar la observancia de las normas teóricamente existentes en el departamento de Información y Tecnología y su coherencia con las del resto de la empresa.
- Determinar las posibles vulnerabilidades de seguridad de la información en el ambiente informático de la ONG.

Alcance de los Objetivos:

Verificar la eficiencia de las operaciones en las áreas funcionales, consistirá en la revisión de los Controles Técnicos Generales de Operatividad, para verificar la compatibilidad de funcionamiento simultáneo del Sistema Operativo y los Aplicativos existentes, incluyendo el hardware y software; y los Controles Técnicos Específicos de Operatividad, el cual incluirá los parámetros de asignación de espacio en disco mínima, periodos de retención de carpetas comunes a varios Aplicativos en cada una de las áreas funcionales.

Verificar la observancia de las normas teóricamente existentes en el departamento de Información y Tecnología y su coherencia con las del resto de la empresa, refiriéndose a la revisión inicial de las normas de instalación informática, sin concentrarse en las contradicciones existentes, pero registrando las áreas que carezcan de normativa; verificación de procedimientos generales informáticos; revisión de los procedimientos específicos informáticos y su concordancia con los procedimientos generales.

Determinar las posibles vulnerabilidades de seguridad de la información en el ambiente informático de la ONG, conociendo la situación actual del ambiente informático y capital humano, verificando conocimientos de integridad, confidencialidad y confiabilidad de la información mediante la formulación de cuestionarios, de tal modo que se puedan reducir riesgos y aumentar controles que se encuentran definidos en el estándar pero que no están siendo implementados.

2.2. Revisión documental

Se requiere el Sistema de Gestión de la Seguridad de la Información (SGSI) como documentación principal de revisión bajo los criterios de auditoría. De manera específica, ISO 27001:2013 indica [3] que un

SGSI debe contener documentos, sin importar el tipo de medio o formato, tales como:

Alcance del SGSI: espacio comprendido dentro de los límites determinados por la organización que estará regido bajo el SGSI, la cual incluye detalladamente cada una de las dependencias, relaciones y límites existentes entre el alcance y aquellas partes que no hayan sido consideradas, sean estas tareas concretas, aplicativos, procesos, departamentos o delegaciones.

Política y objetivos de seguridad: el mismo que especificará cuál es el compromiso de la dirección dentro del Sistema de Gestión de la Seguridad de la Información, adicionando el enfoque primario de la organización en la gestión.

Procedimientos y mecanismos de control que soportan al SGSI: métodos o sistema estructurado que será utilizado para la regulación del funcionamiento del SGSI.

Enfoque de evaluación de riesgos: detalle de cada metodología que será empleada y la ampliación de los criterios de riesgos

(especificando cómo hacer las distintas evaluaciones de las amenazas, probabilidades de ocurrencia e impactos, y vulnerabilidades en cada uno de los activos de información identificados en el alcance), se debe definir niveles de riesgos aceptables.

Reporte de evaluación de riesgos: resultado obtenido tras haber evaluado, mediante la metodología definida, a cada uno de los activos de información de la organización.

Programa de tratamiento de riesgos: documento en el cual se detallan aquellas acciones de la dirección, de los recursos, y cada una de las responsabilidades y prioridades que se llevaran a cabo para poder resolver cada riesgo encontrado de seguridad de la información; todo esto debe estar basado en gran parte en los objetivos de control identificados, y específicamente por los recursos disponibles y conclusiones obtenidas en el reporte de evaluación de riesgos.

Documentación de procedimientos: cada uno de los documentos que avalan la seguridad de la información a través de la planificación,

operación y control de procesos, incluyendo control de índices de eficacia de controles de referencia implantados.

Registros: todos los escritos que proporcionen evidencia alguna de aceptación y conformidad de requisitos y funcionamiento del SGSI.

Proclamación de aplicabilidad: con fin de justificar inclusiones y exclusiones; es todo registro que define los objetivos de control y todos aquellos controles que están estipulados por el SGSI, fundamentados en los hallazgos de los procesos de evaluaciones y tratamiento de riesgos.

2.3. Preparación de auditoría en sitio

La definición de los Objetivos de control y Controles de referencia que serán utilizados durante la Auditoría de la ONG se encuentra en el Anexo 1, cumpliendo con el alcance y parámetros de auditoría ya especificados.

Una vez identificados los Objetivos de control y Controles de referencia, considerados de mayor impacto y detallados en el Anexo 1, estamos listos para realizar la auditoría en sitio.

2.4. Auditoría en sitio

Junta de apertura: Celebrada con la participación de Dirección, el Gerente de Información y Tecnología, el Auditor Contable Interno y el auditor autorizado, se procede con la resolución de dudas del proceso, se presentan a cada uno de los involucrados, incluyendo la persona auditora autorizada y se establecen las condiciones de confidencialidad y medios de comunicación de los resultados.

Ejecución del Plan de Auditoría: Se realizan las observaciones, entrevistas y revisiones necesarias para cubrir con los criterios de auditoría por cada objetivo de referencia de cada objetivo de control, a continuación detallado:

Políticas para la seguridad de la información

Requerimiento para Objetivo de Referencia A.5.1.1: Se solicita la Política de Seguridad de la Información debidamente aprobada, la cual detallará: la definición de seguridad de la información, los objetivos y principios para guiar todas las actividades relacionadas con seguridad de la información; la asignación de las responsabilidades generales y específicas a los distintos roles previamente definidos. La política de seguridad de la información deberá contar al menos con temas que incluyan el control de acceso, clasificación y manejo de la información,

seguridad física y del entorno, una sección de orientación para el usuario final, respaldos, transferencia de información, protección contra malware, administración de vulnerabilidades técnicas, controles criptográficos, seguridad de comunicaciones, y privacidad y protección de información personal. Se requiere un documento de aceptación de comunicación de la presente política a los empleados de la ONG.

Resultado: No conformidad. La documentación se detalla bajo el nombre de Manual de Campo y sólo detalla especificaciones técnicas de configuración de equipos, tales como rangos de IP específicos para determinados servidores y equipos con altos privilegios, definición del tercer octeto a utilizar como agencia ubicada en Guayaquil, conductas de comunicación cuando se está fuera de la organización, nomenclatura de nombre de equipos, nomenclatura de correo electrónico, escasa información sobre configuración de firewall y aplicativo antivirus. Se refiere que las configuraciones son realizadas remotamente por casa matriz. No existe documentación de compartición de información con el resto del personal.

Revisión de las políticas para la seguridad de la información

Requerimiento para Objetivo de Referencia A.5.1.2: Se solicita evidencia de control de revisión, teniendo en cuenta la existencia de un responsable de la administración del desarrollo, revisión y

evaluación de las políticas. La revisión deberá incluir la sección de mejora continua de las políticas en base a cambios del ambiente organizacional, circunstancias del modelo de negocio, condiciones legales o técnicas.

Resultado: No conformidad. El manual de campo es actualizado con una frecuencia promedio de dos años. No se incluye una sección de mejora continua global, se la maneja de manera particular en el uso de rangos de direcciones IP.

Roles y responsabilidades para la seguridad de la información

Requerimiento para Objetivo de Referencia A.6.1.1: Se requiere documentación que evidencie: activos y procesos de seguridad de la información debidamente identificados y asignados; la entidad responsable por cada activo o proceso de seguridad de la información debidamente asignado, documentando el detalle de sus responsabilidades; niveles de autorización definidos y documentados; documentación de que las personas designadas deben ser competentes en el área de la seguridad de la información y cumplan con sus responsabilidades, se debe tener en cuenta que deben tener acceso a las mejoras realizadas; identificación y documentación de coordinación y vigilancia de aspectos de seguridad de la información con respecto a terceros.

Resultado: No conformidad. La organización tiene al Gerente de Información y Tecnología como único responsable del desarrollo e implementación de la seguridad de la información y el debido soporte de los controles respectivos. (Se sugiere que la responsabilidad sobre los recursos y la implementación de los controles caigan sobre cada empleado, protegiendo día a día cada uno de sus activos a cargo).

Segregación de responsabilidades

Requerimiento para Objetivo de Referencia A.6.1.2: Se solicita el manual de funciones detallado de los cargos de la ONG, poniendo especial énfasis en las actividades relacionadas con activos y niveles de supervisión.

Resultado: No conformidad. El manual no menciona las actividades a nivel de detalle. Las funciones se describen de manera general y no se puede verificar la interacción con los activos. El nivel de supervisión se detalla como un organigrama de superior - subordinado. (Se recomienda tomar en cuenta el control como un método de reducir el riesgo accidental o mal uso deliberado de un activo de la organización).

Contacto con las autoridades

Requerimiento para Objetivo de Referencia A.6.1.3: Se requiere evidencia de procedimientos que detallen cuándo y a quién de las autoridades se debe contactar para notificar incidentes que atenten a la seguridad de la información en un tiempo prudencial.

Resultado: No conformidad. La documentación presentada sólo refiere a incidentes o accidentes de tipo humano. No existe documentación que refiera, por ejemplo, a quién recurrir en caso de presentarse un ataque informático. (Se sugiere mantener una documentación apropiada de contactos, sería de gran ayuda como soporte a la continuidad del negocio y los planes de contingencia).

Política para dispositivos móviles

Requerimiento para Objetivo de Referencia A.6.2.1: Se solicita evidencia de registro de dispositivos móviles; requerimientos para protección física; restricción de instalación de aplicativos; requerimientos de versión de aplicativos en dispositivos móviles y aplicación de actualizaciones/parches; restricción de conexión a servicios de información; controles de acceso; técnicas de criptografía; protección de malware; desactivación remota, supresión o bloqueo; respaldos; y uso de servicios y aplicaciones bajo plataforma web.

Resultado: No conformidad. Sólo hay documentación de la existencia de los dispositivos móviles, para su correspondiente código de activo y registro de los datos de factura. (Se recomienda tener por separado el uso de dispositivos móviles para uso personal y laboral, incluyendo aplicativos que ayuden a dicha segmentación con el fin de proteger los datos de la organización en el dispositivo privado. El acceso a la información laboral a través de dispositivos móviles debe darse únicamente luego de haber firmado un acuerdo de conocimiento de responsabilidades, las cuales incluyen protección física y actualización de aplicativos, renunciando a ser propietario de los datos de la empresa, permitiendo limpieza remota de datos en caso de robo, pérdida del dispositivo, o desautorización del uso del mismo. Tener en cuenta que la información almacenada en dispositivos móviles podrían no ser respaldados bajo el escenario de limitaciones de ancho de banda en la red o porque el dispositivo puede no estar encendido en los horarios establecidos para respaldos).

Teletrabajo

Requerimiento para Objetivo de Referencia A.6.2.2: Se requiere la política de condiciones y restricciones para la realización de actividades bajo modalidad de teletrabajo. Se considera la existencia de seguridad física del sitio en donde se realizan las actividades; los

requerimientos de seguridad en las comunicaciones; la provisión de acceso por escritorio remoto; y protección contra malware y requerimientos de firewall.

Resultado: No conformidad. Los equipos tienen instalado únicamente el aplicativo antivirus para personas que trabajan bajo esta modalidad. (Se sugiere provisionar equipos debidamente configurados y dispositivos de almacenamiento para actividades de teletrabajo, en donde se garantice que equipos no autorizados no puedan conectarse a los aplicativos de la organización; la información a la que tenga acceso deberá estar debidamente clasificada y protegida; acceso remoto seguro debería ser provisionado; seguridad física; procesos de respaldo y continuidad de negocio; y monitoreo continuo de seguridad).

Términos y condiciones del empleo

Requerimiento para Objetivo de Referencia A.7.1.2: Se requieren los acuerdos de confidencialidad o no divulgación de todos los empleados; las responsabilidades por la clasificación de la información y la administración de activos organizacionales asociados con información; responsabilidades del empleado por el manejo de información recibida por terceros; y las acciones a ejecutarse en caso de violación de acuerdos.

Resultado: Oportunidad de mejora. La organización mantiene las especificaciones de acuerdos de confidencialidad y no divulgación embebidas en el contrato, y adicionalmente descritas en el reglamento interno. Todo empleado antes de ingresar a laborar firma el documento de acuerdos y condiciones concernientes a seguridad de la información.

Responsabilidades de la dirección

Requerimiento para Objetivo de Referencia A.7.2.1: Se requiere evidencia de políticas y procedimientos que indiquen que todos los empleados están debidamente informados de sus roles y responsabilidades bajo seguridad de la información previo a la obtención de acceso a información confidencial o uso de sistemas de información; y apropiados métodos de trabajo.

Resultado: No conformidad. No se evidencia documentación que integre definición de roles y responsabilidades bajo seguridad de seguridad de información. (Se recomienda tener en cuenta que el no tener los roles y responsabilidades definidas, puede causar considerable daño a la organización. Recordar que si el personal está motivado se puede obtener un comportamiento laboral que cause menos incidentes en cuanto a seguridad de la información).

Toma de conciencia, educación y formación en la seguridad de la información

Requerimiento para Objetivo de Referencia A.7.2.2: Se requiere evidencia de un programa de sensibilización en el tema de seguridad de la información de personal interno como de terceros.

Resultado: No conformidad. Se cuenta con un proceso de inducción que se da al momento de que el colaborador es contratado; sin embargo no hay un plan de refuerzo continuo y no existe una prueba de finalización para medir los conocimientos adquiridos. (Se sugiere tener en cuenta que el entrenamiento puede realizarse en una sala de clase, a distancia, basado en web, autoaprendizaje y otros; el detalle está en que se cubran temas como el compromiso de todos con respecto a la seguridad de la información; la necesidad de familiarizarse con las reglas y obligaciones de la seguridad de la información definidas en políticas, estándares, leyes, regulaciones, contratos y acuerdos; responsabilidad por las acciones e inacciones tomadas en cuando a protección de la información, incluyendo el monitoreo hacia terceras personas; plan de comunicación de incidentes y conceptos generales de procedimientos de seguridad, como por ejemplo la seguridad de las contraseñas, malware y escritorios limpios; puntos de información en dónde se pueda consultar

nuevas formas o mecanismos de protección con el fin de mejorar continuamente los conocimientos ya adquiridos).

Inventario de activos

Requerimiento para Objetivo de Referencia A.8.1.1: Se pide evidencia de documentación de activos relevantes en el ciclo de vida de la información con su importancia debidamente registrada.

Resultado: No conformidad. Se mantiene un documento que detalla todos los activos de la fundación, en dónde la importancia está regida por el costo monetario del mismo, más no por el impacto en el ciclo de vida de la información. (Se recomienda considerar que el documento que detalla el ciclo de vida de información debe incluir desde la creación, el procesamiento, el almacenamiento, la transmisión, la eliminación y la destrucción; éste debe estar debidamente actualizado, ser consistente y registrar siempre el responsable).

Propiedad de los activos

Requerimiento para Objetivo de Referencia A.8.1.2: Se pide evidencia del proceso de asignación de activos, así como la documentación respectiva.

Resultado: No conformidad. Los activos están asignados a un responsable, pero no se garantiza que estén siendo debidamente

protegidos. (Se sugiere tener presente que el responsable debe asegurar que el activo esté inventariado; asegurar que el activo esté debidamente clasificado y protegido; definir y periódicamente revisar las restricciones de acceso y clasificación de los activos más importantes teniendo en cuenta las políticas de control de acceso definidas; y asegurar apropiado manejo cuando el activo es eliminado o destruido)

Uso aceptable de los activos

Requerimiento para Objetivo de Referencia A.8.1.3: Se requiere el documento de reglas para el uso aceptable de información y de activos asociados con información, se debe evidenciar las facilidades de procesamiento de la información debidamente identificada, documentadas e implementadas.

Resultado: No conformidad. El personal es responsable por varios activos, pero no necesariamente son de información. (Se recomienda que empleados y terceros que tengan acceso a la organización sean concientizados sobre las políticas de seguridad de la información, responsabilizándolos por su uso durante el tiempo que estén vinculados a la organización).

Devolución de activos

Requerimiento para Objetivo de Referencia A.8.1.4: Se requiere evidencia de recepción de activos de información al culminar el vínculo con la organización.

Resultado: No conformidad. Se observa documento de recepción de activos físicos, más no se constata documentación de recepción de activos de información. (Se sugiere considerar que la terminación del proceso debería ser formalizada una vez se hayan recibido todos los activos de información y electrónicos que la organización otorgó en su momento al empleado o terceros. Si se ha utilizado equipos personales, la información que se maneje en estos equipos deberá ser transferida al término de la actividad. Durante el periodo de terminación la organización debe tener control sobre la copia no autorizada de información relevante de la organización).

Clasificación de la información

Requerimiento para Objetivo de Referencia A.8.2.1: Se requiere evidencia de clasificación de información.

Resultado: No hay evidencia. (Nota: tener presente que la clasificación provee a los empleados o terceros que manejan información de manera concisa cómo manipularla y protegerla).

Etiquetado de la información

Requerimiento para Objetivo de Referencia A.8.2.2: Se requiere evidencia de procedimiento para etiquetado de la información.

Resultado: No hay evidencia. (Nota: Considerar que el etiquetado de la clasificación de la información es clave para los acuerdos de compartición de información. Se sugiere etiquetados físicos y metadato, son una común forma de identificar. Siempre teniendo en cuenta que el etiquetado deja en evidencia los activos valiosos y pueden ser sujetos a robo por personal interno o por terceros).

Manejo de activos

Requerimiento para Objetivo de Referencia A.8.2.3: Se requiere la documentación de procedimientos de manejo, procesamiento, almacenamiento y comunicación de información consistente con su clasificación.

Resultado: No conformidad. Sólo se mantiene un registro formal de activos de recipientes autorizados. (Se sugiere incluir las restricciones de acceso para el apoyo de requerimientos de protección por cada nivel de clasificación; protección de copias de información, temporal o permanente, a un nivel consistente con la protección de información original; almacenamiento de activos de TI en acuerdo con las

especificaciones de fábrica; marcado claro de todas las copias de medios para la atención del recipiente autorizado).

Gestión de medios removibles

Requerimiento para Objetivo de Referencia A.8.3.1: Se solicita evidencia de procedimientos para la gestión de medios removibles.

Resultado: No conformidad. Sólo existe un procedimiento para el escenario de donación o desecho de activos, el cual refiere a un borrado de información previa. (Se sugiere reforzar el procedimiento con guías para asegurar que medios removibles no requeridos, deben de estar bajo un proceso de borrado de información no recuperable; en caso de ser necesario y práctico, la autorización debe ser requerida para la eliminación de los mismos dejando un registro de dichos medios para efectos de auditoría; todos los medios removibles deberían ser almacenados en un lugar seguro bajo las especificaciones de fábrica; en caso de ser necesario por efectos de confidencialidad o integridad en algunos datos, se debería utilizar técnicas de criptografía para proteger los datos en medios removibles; para evitar el riesgo de daño mientras la información es aún necesaria, la data debería ser transferida a un medio extraíble nuevo antes de que se vuelva difícil de leer en el anterior, todo esto debidamente monitoreado; en caso de datos importantes se debería tener múltiples

copias y almacenarlas en medios separados y apartados con el fin de reducir el riesgo de pérdida o daño de datos; registro de medios removibles deberían ser mantenidos para limitar posibles pérdidas de datos; tener en consideración que los medios removibles únicamente deben ser habilitados si existe alguna razón justificada para hacerlo).

Eliminación de los medios

Requerimiento para Objetivo de Referencia A.8.3.2: Se requiere documentación de procedimientos formales para la correcta eliminación de medios.

Resultado: No conformidad. La documentación mostrada sólo refiere a procedimientos de eliminación de discos duros bajo técnicas de borrado de información. (Se sugiere modificar la guía y agregar mayor detalle acerca del manejo de medios con información confidencial a ser eliminados, manteniéndolos en un lugar seguro y eliminándolos de forma segura; se debería clasificar aquellos medios que tengan información sensible para una rápida identificación y una segura eliminación; si se dispone de algún servicio de retiro y eliminación de medios, se debe tener cuidado en la selección del tercero, el cual debe tener experiencia verificable en la ejecución de lo requerido; todo medio a ser eliminado debería ser registrado para efectos de auditoría; se debe tener presente que todo medio dañado que contenga datos

sensibles deben ser sometidos a decisión para ver si es mejor arreglarlos antes que eliminarlos).

Transferencia de medios físicos

Requerimiento para Objetivo de Referencia A.8.3.3: Se requiere evidencia de guías consideradas para proteger los medios que contienen información sensible de acceso no autorizado.

Resultado: No hay evidencia. (Se sugiere documentar una guía que incluya aspectos como servicios seguros de transportación o correo; una lista autorizada de entidades que presten servicio de correo previamente autorizada; procedimientos para verificar la identificación de entidades de correo; guías de empaquetado con el fin de evitar algún daño físico durante la transportación del medio en acuerdo con las especificaciones de fábrica; los registros de log deberían ser mantenidos, identificando el contenido del medio, la protección aplicada, así como registrar el número de veces que ha sido sujeto a transferencia, evidenciando el custodio inicial y final; si los datos no están encriptados, se debería adoptar un mecanismo de protección física adicional).

Política de control de acceso

Requerimiento para Objetivo de Referencia A.9.1.1: Se requiere documentación de la política de control de acceso, la misma deberá

estar establecida, documentada y revisada según los requerimientos de la organización.

Resultado: No conformidad. La política refiere únicamente procedimientos de seguridad en las aplicaciones del negocio. (Se sugiere se tome en cuenta aspectos como políticas de diseminación y autorización; consistencia entre los derechos de acceso y la clasificación de información tanto en aplicativos como red interna; legislación relevante y cualquier obligación contractual establecida que requiera acceso a datos o servicios; administración de derechos de acceso en un ambiente distribuido y conectado que reconozca todos los tipos de conexiones disponibles; segregación de roles en cuanto a control de acceso; requerimientos formales para solicitar acceso; proceso de revisión de la política de derechos de acceso y retiro de los mismos; registro de eventos significativos concernientes al uso y administración de identidades de usuarios e información de autenticación).

Acceso a redes y a servicios en red

Requerimiento para Objetivo de Referencia A.9.1.2: Se solicita política de acceso a redes y a servicios en red.

Resultado: Oportunidad de mejora. La documentación incluye la segmentación de red a utilizar por cada establecimiento, incluyendo la

política de parámetros y configuraciones a considerar en el enlace de datos; se evidencia guías de permisos sobre unidades de red compartidas y varias configuraciones de restricciones sobre cambios a realizar en los propios equipos; existen procedimientos para el uso de VPN o redes inalámbricas. (Se sugiere tener en cuenta algún mecanismo propio que les permita monitorear el uso de los servicios de red).

Registro y cancelación del registro de usuarios

Requerimiento para Objetivo de Referencia A.9.2.1: Se requiere evidencia de solicitudes de petición de registros y cancelaciones de usuarios sobre acceso a aplicativos y servicios.

Resultado: No hay evidencia. (Se sugiere desarrollar una política de petición de registro de nuevos usuarios y de cancelación de usuarios que ya no mantienen vínculo alguno con la organización; el uso de identificadores de usuarios únicos, el cual será vinculado a los distintos aplicativos y servicios manteniendo responsabilidad absoluta sobre las acciones tomadas sobre los mismos; monitorear la lista de usuarios ya registrados con el fin de monitorear posible duplicidad de identificadores).

Suministro de acceso de usuarios

Requerimiento para Objetivo de Referencia A.9.2.2: Se requiere evidencia de un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.

Resultado: No hay evidencia. (Se recomienda establecer una política de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios, ya sea que se requiera acceso a aplicativos o a servicios, los mismos deberán cubrir aspectos como verificar el nivel de acceso que será otorgado el cual debe de ser consistente con las responsabilidades asociadas a cada usuario; asegurar que los derechos de acceso no deben ser otorgados antes de que se hayan completado los procedimientos de autorización; mantener un registro de accesos otorgados a cada usuario por sistema de información y servicio; manejar la adaptabilidad de permisos en caso de cambio de roles o posiciones, teniendo en cuenta el correspondiente bloqueo o revocación a aquellos accesos que no serán utilizados; mantener un monitoreo constante sobre los permisos que se hayan otorgado para acceder a sistemas de información o servicios).

Gestión de derechos de acceso privilegiado

Requerimiento para Objetivo de Referencia A.9.2.3: Se requiere evidencia de gestión de derechos de acceso privilegiado mediante un proceso formal de autorizaciones en acuerdo con la política de control de acceso.

Resultado: No hay evidencia. (Se sugiere establecer una política formal de gestión de derechos de acceso privilegiado, contemplando temas como identificación de derechos de acceso privilegiados asociados con cada aplicativo o proceso, y los usuarios a quienes se les necesite asignar permisos bajo estricto control basado en requerimientos mínimos para el correcto desempeño de sus roles funcionales; contemplar historial de registros de los privilegios asignados; definición de requerimientos por expiración de derechos de acceso privilegiados otorgados; revisión de competencia de usuarios con derechos de acceso privilegiados con el fin de verificar que estén alineados con sus responsabilidades; procedimientos específicos deberían ser establecidos y mantenidos para evitar el uso no autorizado de administración genérica de identificadores de usuario; en caso de autenticación genérica, se deberá tener en cuenta la confidencialidad al momento de compartirla).

Gestión de información de autenticación secreta de usuarios

Requerimiento para Objetivo de Referencia A.9.2.4: Se requiere documentación de proceso de administración formal de asignación de información de autenticación.

Resultado: No hay evidencia. (Se recomienda una guía de administración formal de asignación de información de autenticación que incluya aspectos como acuerdos firmados de mantener la información de autenticación de manera confidencial, en caso de información de autenticación grupal, dicho acuerdo debe ser firmado por todos los miembros; cada usuario debe tener inicialmente una clave temporal para poder acceder y debe cambiarla luego de su primer uso; establecimiento de procedimientos para verificar la identidad de un usuario antes de proveer una nueva clave, una recuperación de contraseña o una clave temporal; las claves temporales deben ser enviadas de manera segura, métodos de terceros o correos electrónicos deberían ser evitados; las claves temporales deberían ser únicas para cada individuo y no ser de fácil adivinación; todos los usuarios deberían estar familiarizados con las políticas y firmar un acta de conocimiento de la misma; el uso de claves criptográficas y *tokens* podría ser considerado).

Revisión de los derechos de acceso de usuarios

Requerimiento para Objetivo de Referencia A.9.2.5: Se requiere evidencia de revisión de documentación de derechos de acceso de usuarios.

Resultado: No hay evidencia. (Se recomienda que la documentación de derechos de acceso de usuarios sea revisada a intervalos regulares luego de cualquier cambio; los permisos de usuario deberían ser revisados y reasignados en especial cuando se realizan cambios de rol; las autorizaciones para derechos de acceso privilegiados deberían también ser revisadas con regularidad; considerar mantener un historial de cambios para efectos de auditoría, es muy útil).

Retiro o ajuste de los derechos de acceso

Requerimiento para Objetivo de Referencia A.9.2.6: Se requiere evidencia de los retiros o ajustes de los derechos de acceso.

Resultado: No hay evidencia. (Se recomienda que se lleve un control documentado del retiro o ajustes de los derechos de acceso, en especial cuando ya se haya terminado un vínculo entre la organización y un empleado o terceras personas; tomando en cuenta no sólo el acceso lógico, sino también el acceso físico; la comunicación de personas que ya no forman parte de la organización, en especial si se

tiene un grupo, es indispensable, puesto que, es necesario que se manifieste que ya no se deberá seguir compartiendo información).

Uso de información de autenticación secreta

Requerimiento para Objetivo de Referencia A.9.3.1: Se requiere evidencia de uso de información de autenticación secreta.

Resultado: No hay evidencia. (Se recomienda compartir con el personal o terceros que necesiten acceder a la información, que deben de cumplir con las prácticas de uso responsable de la información de autenticación, enfatizando aspectos como mantener en secreto toda información confidencial de autenticación, asegurando que no sea divulgada a ninguna entidad, incluyendo personal de autoridad; evitar mantener un registro en papel, programas, archivos, o dispositivos de mano de información de autenticación, a menos que pueda ser mantenida de manera segura y el método de almacenamiento sea aprobado; realizar el cambio de contraseña con regularidad y más aún si se sospecha que la clave está comprometida; las contraseñas deberían ser fáciles de recordar para el usuario (no deberán ser basadas en algo o alguien que fácilmente de indicios para poderla adivinar debido a supuestas relaciones), no vulnerables ante un ataque de diccionario, no deberán estar compuestas por sólo letras o sólo números; si la clave otorgada es temporal, deberá ser cambiada

luego del primer uso; no debe compartir su clave de autenticación; asegurarse de que su clave no sea guardada automáticamente bajo ninguna plataforma; considerar no usar claves viejas por ningún motivo).

Restricción de acceso a la información

Requerimiento para Objetivo de Referencia A.9.4.1: Se requiere documentación que evidencia la política de control de acceso en cuanto a la restricción a la información.

Resultado: No hay evidencia. (Se recomienda establecer políticas de restricción de acceso basadas en requerimientos individuales de aplicativos de la organización en acuerdo con las políticas de control definidas. Se debe considerar aspectos como menú para controlar el acceso a las funciones de los aplicativos; controlar que dato puede ser accedido por cada usuario; controlar el derecho de acceso de usuarios bajo lectura, escritura, eliminación y ejecución; controlar el acceso hacia otras aplicaciones; limitar el contenido de información en los reportes; proveer controles de acceso físicos y lógicos hacia aplicaciones sensibles, datos o sistemas internos).

Procedimiento de ingreso seguro

Requerimiento para Objetivo de Referencia A.9.4.2: Se requiere evidencia de política de control de acceso a sistemas y aplicaciones, controladas por un procedimiento seguro de inicio de sesión.

Resultado: No conformidad. Se evidencia que existe un proceso de autenticación; sin embargo, no se evidencia seguridad en el mismo. (Se recomienda agregar una técnica de autenticación acorde que involucre verificación de identidad de usuario, algunos ejemplos son métodos criptográficos, tarjetas inteligentes, *tokens* o biométricos. Tener en cuenta que el procedimiento de autenticación a un sistema o aplicativo debe ser diseñado para minimizar la oportunidad a que usuarios no autorizados tengan acceso, algunos aspectos a considerar pueden ser el no mostrar evidencia alguna de anteriores usuarios autenticados; no mostrar información parcial hasta que se haya completado el proceso como tal; mostrar un mensaje general de que el computador debe ser accedido únicamente por usuarios autorizados; ante cualquier fallo de autenticación el sistema no debe indicar que parte en específico fue la que ocasionó el fallo; mantener protección en contra de mecanismos como fuerza bruta; mantener un historial de autenticaciones exitosas y no exitosas; levantar un evento de seguridad si se identifica un comportamiento comprometido en el proceso de autenticación; se debe mostrar para el escenario de

autenticación exitosa datos como fecha y hora de la última conexión y detalles de cualquier autenticación no exitosa desde la última conexión exitosa realizada; tener en cuenta que jamás se debería mostrar la contraseña en el campo respectivo; considerar no permitir la transmisión de contraseñas en texto plano sobre la red; cerrar sesiones inactivas luego de un tiempo prudencial; y definir horario de conexiones restringidas con el fin de disminuir el alto riesgo por conexiones no autorizadas).

Sistema de gestión de contraseñas

Requerimiento para Objetivo de Referencia A.9.4.3: Se requiere evidencia de gestión de contraseñas.

Resultado: No conformidad. Existe una gestión de contraseñas pero no incluye el refuerzo de seleccionar claves de calidad o de cambiar las contraseñas con regularidad. (Se sugiere tomar en consideración aspectos como el refuerzo de que el uso de los identificadores y las claves son personales; permitir al usuario seleccionar y cambiar sus propias contraseñas e incluir una confirmación de culminación de procedimiento; no mostrar la contraseña en la pantalla; guardar los archivos de contraseñas lejos del lugar en donde se encuentren los datos; la transmisión y almacenamiento de las contraseñas se debe realizar de manera segura; reforzar la selección de claves de calidad;

y considerar mantener un registro de contraseñas utilizadas para prevenir el reúso de las mismas).

Uso de programas de utilidad privilegiados

Requerimiento para Objetivo de Referencia A.9.4.4: Se requiere documentación que evidencie restricciones en el uso de programas de utilidad privilegiados.

Resultado: No hay evidencia. (Se recomienda establecer una política de restricciones en el uso de programas utilitarios que tome en cuenta controles sobre el uso de identificación, autenticación y procedimientos de autorización para programas de utilidad; segregación de programas de utilidad y otras aplicaciones; limitación del uso de programas de utilidad a un mínimo número práctico de usuarios confiables y autorizados; autorización de uso especial de programas de utilidad; limitación de disponibilidad de programas de utilidad; autenticación implementada en todo programa de utilidad; definir y documentar niveles de autorización; y tener en mente el desinstalar o deshabilitar todo programa de utilidad innecesario).

Control de acceso a código fuente de aplicativos

Requerimiento para Objetivo de Referencia A.9.4.5: Se requiere evidencia de que existe un control de acceso a código fuente de aplicativos.

Resultado: No conformidad. Sólo aplicativos bajo plataforma web se mantienen con restricciones de acceso a código fuente, aplicativos de escritorio locales no mantienen control alguno. (Se sugiere elevar los controles de restricción teniendo en cuenta los siguientes aspectos, donde sea posible, las librerías fuentes de los programas no deben estar almacenados en los sistemas operativos; el código fuente y las librerías deben ser administradas acorde a procedimientos establecidos; el personal de soporte no debe tener acceso no restringido al código fuente o librerías; las actualizaciones de los programas deben realizarse una vez se tenga la autorización correspondiente; considerar que el historial de accesos a los códigos fuentes y librerías debe ser realizado; el mantenimiento y copia del código fuente debe ser sujeto a procedimientos de control de cambios estrictos).

Política sobre uso de controles criptográficos

Requerimiento para Objetivo de Referencia A.10.1.1: Se requiere documentación de política de uso de controles criptográficos.

Resultado: No hay evidencia. (Se sugiere desarrollar una política de uso de controles criptográficos teniendo en cuenta aspectos como el enfoque de gestión hacia el uso de controles criptográficos en toda la organización, incluyendo los principios generales en las que la información de negocios debe ser protegida; identificar el nivel de protección, teniendo en consideración el tipo, la robustez y la calidad del algoritmo de encriptación requerido; el uso de encriptación para protección de la información transportada por medios móviles o dispositivos removibles, o por otras líneas de comunicación; el enfoque de la gestión de claves, incluyendo métodos para hacer frente a la protección de claves criptográficas y la recuperación de la información codificada en el caso de pérdida de llaves; generar roles y responsabilidades de la administración de claves; considerar el impacto de usar información encriptada en controles que dependen de inspección de contenido).

Administración de llaves

Requerimiento para Objetivo de Referencia A.10.1.2: Se requiere evidencia de documentación de administración de llaves.

Resultado: No hay evidencia. (Se recomienda desarrollar una política de documentación de administración de llaves, que incluya todo el ciclo de vida, es decir, generación, almacenamiento, recuperación,

distribución, retiro y destrucción; tener en cuenta la selección del largo de las claves, así como el algoritmo criptográfico respectivo; toda llave criptográfica debe estar protegida contra modificación y pérdida; llevar historial de actividades relacionadas a claves criptográficas para efectos de auditoría).

Perímetro de seguridad

Requerimiento para Objetivo de Referencia A.11.1.1: Se requiere documentación que evidencie perímetros de seguridad sobre información confidencial o crítica.

Resultado: No conformidad. (Se sugiere el desarrollo de una política de seguridad perimetral definida y usada para proteger áreas que contengan información crítica o sensible, teniendo en cuenta que barreras físicas, en donde aplique, deben ser construidas para prevenir acceso físico no autorizado y contaminación del área por el ambiente; todas las puertas de salida en caso de incendio deberán tener alarma en caso de encontrarse dentro del perímetro de seguridad, considerar que deben ser monitoreadas y probadas; sistemas de detección de intrusos deben ser incorporados para complementar la seguridad; las instalaciones físicas del procesamiento de información debe estar separado de aquellos espacios administrados por terceras personas).

Controles de acceso físicos

Requerimiento para Objetivo de Referencia A.11.1.2: Se requiere evidencia de documentación que incluya controles de acceso físicos.

Resultado: No conformidad. (Se sugiere tener en cuenta los siguientes aspectos en la documentación actual, la fecha y hora de entrada y salida de visitantes debe ser supervisada y registrada; el acceso a las áreas en donde información confidencial es procesada o almacenada debe ser restringida a personal no autorizado; todo empleado o tercera persona debe vestir una identificación visible que permita llevar un control sobre individuos que estén dentro del perímetro restringido; toda tercera persona debe tener autorización para poder ingresar al área restringida; la política debe ser revisada con regularidad y actualizada cuando sea necesario).

Seguridad de oficinas, recintos e instalaciones

Requerimiento para Objetivo de Referencia A.11.1.3: Se requiere evidencia de seguridad de oficinas, recintos e instalaciones.

Resultado: No conformidad. (Se recomienda tener en cuenta dentro de la política que las instalaciones claves deberían estar situadas estratégicamente para evitar el acceso de personal no autorizado; donde sea aplicable, se deberá establecer el entorno de tal forma que actividades que involucren información confidencial no puedan ser ni

visualizadas ni escuchadas por terceros; el directorio y los libros telefónicos internos que identifican localidades de procesamiento de información confidencial no deben ser de fácil acceso para la lectura de personal no autorizado).

Protección contra amenazas externas y ambientales

Requerimiento para Objetivo de Referencia A.11.1.4: Se requiere evidencia de protección contra amenazas externas y ambientales.

Resultado: Oportunidad de mejora. (Se sugiere pedir ayuda a un profesional en cómo evitar daños causados por fuego e inundaciones).

Trabajo en áreas seguras

Requerimiento para Objetivo de Referencia A.11.1.5: Se requiere evidencia de controles para trabajar en áreas seguras.

Resultado: Oportunidad de mejora. (Se recomienda tomar en consideración evitar el trabajo no supervisado en áreas seguras por razones de seguridad y para prevenir oportunidades para la ejecución de actividades maliciosas).

Áreas de despacho y carga

Requerimiento para Objetivo de Referencia A.11.1.6: Se requiere evidencia de control de acceso en áreas de despacho y carga.

Resultado: No conformidad. Los equipos se mantienen al alcance de terceros al momento de recibir y/o entregar pedidos. (Se sugiere tomar en consideración los siguientes aspectos, el acceso al área de carga y despacho debe estar fuera del inmueble principal y con acceso restringido; el área de carga y despacho debe estar diseñada para que personal no autorizado entre en el edificio; todo material que ingrese debe ser registrado en acuerdo con los procedimientos de administración de activos e inspeccionado).

Ubicación y protección de los equipos

Requerimiento para Objetivo de Referencia A.11.2.1: Se requiere evidencia de equipos debidamente ubicados y protegidos.

Resultado: No conformidad. Los equipos no están estratégicamente ubicados, algunos son de libre acceso. (Se recomienda tomar en cuenta aspectos como situar los equipos de tal modo que se reduzca el acceso innecesario al área de trabajo por terceros, permitiéndoles visualizar información que puede ser categorizada como sensible; adoptar controles para reducir el riesgo de problemas potenciales de tipos físico y ambiental; guías para comer, beber, y/o fumar deben ser establecidas bajo escenarios de proximidad con instalaciones de procesamiento de información; las condiciones ambientales, como la

temperatura y la humedad deben ser monitoreadas por condiciones que afecten las operaciones de procesamiento de información).

Seguridad del cableado

Requerimiento para Objetivo de Referencia A.11.2.3: Se requiere evidencia de seguridad del cableado.

Resultado: Oportunidad de mejora.

Mantenimiento de equipos

Requerimiento para Objetivo de Referencia A.11.2.4: Se requiere evidencia de mantenimiento de equipos.

Resultado: Oportunidad de mejora. Se evidencia un plan de mantenimiento semestral en equipos sensibles y no sensibles. (Se recomienda considerar aspectos como las especificaciones de equipos para coordinar la frecuencia del mantenimiento; recordar que sólo el personal autorizado debe llevar a cabo las reparaciones y mantenimientos; se debe llevar una bitácora por equipo en cuanto a mantenimientos preventivos y correctivos; controles apropiados deben ser tomados en cuenta al momento de la ejecución del mantenimiento, en especial si el servicio lo otorga un tercero; antes de devolver el equipo a su lugar asignado, debe ser chequeado con el fin de verificar que no haya sido dañado o intervenido).

Retiro de activos

Requerimiento para Objetivo de Referencia A.11.2.5: Se requiere evidencia de guía para el retiro de activos.

Resultado: Oportunidad de mejora. (Se recomienda tener en cuenta un límite de tiempo para remover activos y la verificación de los mismos al cumplirse el mantenimiento).

Seguridad de equipos y activos fuera de las instalaciones

Requerimiento para Objetivo de Referencia A.11.2.6: Se requiere evidencia de guías de seguridad de equipos y activos fuera de las instalaciones.

Resultado: No conformidad. Se constata almacenamiento de equipos fuera de las instalaciones en condiciones no adecuadas. (Se recomienda que se tenga en consideración que el uso de cualquier dispositivo de almacenamiento de información y equipos fuera de la organización debe ser autorizado por la directora; esto aplicaría también a equipos propios que son utilizados para la organización; considerar el hecho de que no se deben dejar en desatención en ningún momento; en caso de que el equipo sea transferido mientras se encuentre fuera de la organización, se debe llevar una cadena de custodia que detalle el propietario temporal y la organización responsable).

Eliminación segura o reutilización de equipos

Requerimiento para Objetivo de Referencia A.11.2.7: Se requiere evidencia de procedimiento para la eliminación segura o reutilización de los equipos.

Resultado: No conformidad. Se constata disco duro en equipo a ser donado sin la correspondiente eliminación de información. (Se recomienda que los equipos sean verificados para asegurar que los medios de almacenamiento se destinen a su eliminación o a su reúso; tener en cuenta mecanismos de borrado antes de su eliminación o reúso por parte de terceros).

Equipos de usuario desatendido

Requerimiento para Objetivo de Referencia A.11.2.8: Se requiere evidencia de políticas de protección para equipos de usuario desatendido.

Resultado: No hay evidencia. (Se sugiere tener en consideración que todos los usuarios deben de ser advertidos de los requerimientos de seguridad y procedimientos respectivos para equipos desatendidos; así como también sus responsabilidades para implementar dicha protección).

Política de escritorio limpio y pantalla limpia

Requerimiento para Objetivo de Referencia A.11.2.9: Se requiere evidencia de política de escritorio limpio y pantalla limpia.

Resultado: No hay evidencia. (Se sugiere desarrollar una política de escritorio y pantalla limpia teniendo en consideración la clasificación de la información; archivos con información sensible deben ser removidos de las impresoras inmediatamente; computadores y terminales deben ser dejados con la sesión cerrada y protegidos con un protector de pantalla y bloqueo de teclado controlado por una contraseña, *token* o mecanismos similares de autenticación).

Procedimientos de operación documentados

Requerimiento para Objetivo de Referencia A.12.1.1: Se requiere evidencia de documentación de procedimientos de operaciones.

Resultado: No conformidad. Se identificaron dos usuarios que no conocían la ubicación de los procedimientos de operación. (Se recomienda que la documentación de los procedimientos esté desarrollada para actividades operacionales alineadas con el procesamiento de información e instalaciones de comunicaciones; incluyendo la instalación y configuración de aplicativos; procesamiento y manejo de información de manera automática y manual; respaldos; requerimientos agendados, incluyendo interdependencias entre

sistemas internos y externos; considerar las instrucciones para manejo de errores u otras condiciones excepcionales que puedan presentarse durante la ejecución de algún *job*; soporte y contacto de respaldo incluyendo el soporte efectuado por terceros; instrucciones de manejo de medios y resultados especiales, incluyendo eliminación segura de resultados de un *job* fallido; contemplar procedimientos de reinicio y recuperación para el uso de eventos de falla del sistema; la administración de historial de log; monitoreo continuo de procedimientos).

Gestión de cambios

Requerimiento para Objetivo de Referencia A.12.1.2: Se requiere evidencia de gestión de cambios.

Resultado: No hay evidencia. (Se recomienda desarrollar una guía para cambios que ocurran en la organización, procesos del negocio, instalaciones de procesamiento de información y sistemas que puedan afectar la seguridad de la información; identificación y registro de cambios significativos; planeación y pruebas de cambios; evaluación de impactos potenciales, incluyendo impactos de seguridad de la información; considerar un procedimiento formal de aprobación para cambios propuestos; verificación de que los requerimientos de seguridad de la información han sido conocidos; tener en cuenta la

comunicación de detalles de cambios al personal relevante; procedimientos de repliegue, con escenarios de aborto y recuperación de estado anterior).

Separación de los ambientes de desarrollo, pruebas, y operaciones

Requerimiento para Objetivo de Referencia A.12.1.4: Se requiere evidencia de políticas de separación de los ambientes de desarrollo, pruebas, y operaciones.

Resultado: No hay evidencia. (Se sugiere desarrollar un nivel de separación entre lo operacional, lo que está en estado de pruebas, y el ambiente de desarrollo, muy necesario para prevenir problemas operacionales; incluir reglas para la transferencia de aplicaciones de desarrollo a estado operacional, debidamente definidos y documentado; tener presente que los aplicativos en desarrollo y en estado operativo deben de ser ejecutados en diferentes sistemas o procesadores de computadores, y en diferentes dominios o directorios; todo cambio debe ser previamente probado antes de ser aplicado al sistema operacional; sólo a manera de excepción se permitirá realizar pruebas en el ambiente de producción; compiladores, editores y otras herramientas de desarrollo no deben ser accedidas desde sistemas operacionales cuando no sea requerido; mantener diferentes perfiles para nivel operativo y de pruebas; datos sensibles no deben ser

copiados en un ambiente de prueba a menos que controles equivalentes sean proveídos para la etapa de prueba).

Controles contra códigos maliciosos

Requerimiento para Objetivo de Referencia A.12.2.1: Se requiere evidencia de controles de detección, de prevención y de recuperación.

Resultado: No conformidad. No se evidencia la toma de conciencia apropiada de los usuarios, para protegerse contra códigos maliciosos. (Se recomienda que se tome a consideración el hecho de que la protección contra el malware debe estar basada en detección de malware y reparación de aplicativos, advertencia de seguridad de la información y acceso apropiado a los sistemas, y control de gestión de cambios. La política debería incluir un procedimiento formal que prohíba el uso de aplicativos no autorizados; la implementación de controles que prevengan o detecten el uso de aplicaciones no autorizadas; la implementación de controles que prevengan o detecten el uso de sitios de Internet no recomendables; protección contra riesgos asociados con la recepción de archivos y aplicativos, ya sea vía externa o cualquier medio; administración técnica de vulnerabilidades; instalación y actualización regular de detección de malware para escanear computadores y medios como medida de precaución; preparación del plan de continuidad en caso de

presentarse un ataque producido por un malware; aislar ambientes donde se pueda ser víctima de un resultado catastrófico).

Instalación de aplicativos en sistemas operativos

Requerimiento para Objetivo de Referencia A.12.5.1: Se requiere evidencia de guías de control de instalación de aplicativos en sistemas operativos.

Resultado: Oportunidad de mejora. (Se sugiere tener en cuenta los siguientes aspectos, la actualización de los aplicativos y librerías de programas deben ser realizadas por administradores entrenados previamente autorizados; los controles de configuración de los sistemas deben ser utilizados para mantener el control de todos los aplicativos implementados así como la documentación de cada uno; considerar mantener un log para auditorías, el mismo debe contemplar todas las actualizaciones aplicadas; la versión inmediata anterior debe ser mantenida como medida de contingencia).

Gestión de las vulnerabilidades técnicas

Requerimiento para Objetivo de Referencia A.12.6.1: Se requiere evidencia de información acerca de las vulnerabilidades técnicas de los sistemas de información que se usan.

Resultado: No conformidad. Se mantiene una suscripción que informa sobre nuevas vulnerabilidades a nivel general, nada muy detallado. (Se recomienda que se realice un inventario de activos completo como prerrequisito para la administración técnica efectiva de vulnerabilidades. Tomar en cuenta que las acciones apropiadas deben ser tomadas a tiempo en respuesta a la identificación de vulnerabilidades potenciales; la organización debe definir y establecer roles y responsabilidades asociadas con administración de vulnerabilidades, incluyendo el monitoreo, evaluación de riesgo, parche, seguimiento y cualquier otra responsabilidad requerida de coordinación; una vez detectada la vulnerabilidad, la organización debe identificar los riesgos asociados y las acciones a ser tomadas; el riesgo de instalar parches debe ser evaluado antes de cualquier aplicación; considerar que los sistemas con gran riesgo deben ser atendidos primero).

Restricciones sobre la instalación de aplicativos

Requerimiento para Objetivo de Referencia A.12.6.2: Se requiere evidencia de políticas para establecer e implementar las reglas para la instalación de aplicativos por parte de los usuarios.

Resultado: Oportunidad de mejora. (Se sugiere que la organización mejore y haga cumplir la política sobre qué tipos de aplicativos pueden

ser instalados por usuarios; la instalación no controlada de aplicativos puede acarrear grandes consecuencias como la introducción de posibles vulnerabilidades, pérdida de la integridad de la información u otros incidentes de la seguridad de la información).

Controles de redes

Requerimiento para Objetivo de Referencia A.13.1.1: Se requiere evidencia de gestión y control de redes para protección de la información en sistemas y aplicaciones.

Resultado: No conformidad. Se evidencia programa que guarda información de apadrinados sin autenticación y con funcionalidad para realizar modificaciones. (Se sugiere que se incrementen controles para asegurar la seguridad de la información en redes y la protección de servicios conectados de accesos no autorizados; la administración de los equipos de redes deben ser documentados bajo procedimientos de responsabilidades; las responsabilidades operacionales en redes deben estar separadas de las operaciones del computador; controles especiales deben de establecerse para salvaguardar la confidencialidad e integridad de los datos que pasan por las redes públicas; registros de log y monitoreo continuo deberían ser habilitados con el fin de detectar acciones que puedan afectar la seguridad de la información; sistemas utilizados sobre la red deberían

de contar con autenticación; contemplar que la conexión a la red sea restringida).

Seguridad de los servicios de red

Requerimiento para Objetivo de Referencia A.13.1.2: Se requiere evidencia de mecanismos de seguridad de los servicios de red.

Resultado: Oportunidad de mejora. (Se recomienda que siempre se supervise y determine la capacidad del proveedor del servicio de red para gestionar los servicios acordados; es necesario la identificación de medidas de seguridad necesarias para determinados servicios, tales como características de seguridad, niveles de servicio y requisitos de gestión; implementar soluciones como firewalls y sistemas de detección de intrusos).

Separación en las redes

Requerimiento para Objetivo de Referencia A.13.1.3: Se requiere evidencia de control de separación en las redes.

Resultado: Oportunidad de mejora. (Se sugiere que en caso de activar las redes inalámbricas recuerden darle un tratamiento especial debido al pobre perímetro de red definido).

Mensajería electrónica

Requerimiento para Objetivo de Referencia A.13.2.3: Se requiere evidencia de protección adecuada de información incluida en mensajería electrónica.

Resultado: No conformidad. Se evidenció envío de claves en texto plano a través de mensajería instantánea, Skype. (Se recomienda que se considere protección de mensajes de accesos no autorizados, modificaciones o denegación de servicio; asegurar correcto direccionamiento y transportación del mensaje; confiabilidad y disponibilidad de servicio; consideraciones legales para el caso de firmas electrónicas; aprobación previa antes de usar servicios públicos externos como mensajería instantánea, redes sociales o compartición de archivos; fuertes niveles de autenticación de redes públicas).

Acuerdos de confidencialidad o de no divulgación

Requerimiento para Objetivo de Referencia A.13.2.4: Se requiere evidencia de acuerdos de confidencialidad o de no divulgación.

Resultado: No conformidad. El documento de acuerdo existente sólo se aplica a terceros. (Se sugiere que se mejoren los acuerdos de confidencialidad o no divulgación con el fin de proteger la información usando términos de referencia legal; estos acuerdos deben ser aplicados a terceros y empleados de la organización).

Responsabilidades y procedimientos

Requerimiento para Objetivo de Referencia A.16.1.1: Se requiere evidencia de documentación de responsabilidades y procedimientos.

Resultado: No hay evidencia. (Se recomienda desarrollar una guía para administración de responsabilidades y procedimientos considerando planeación y preparación de procedimientos para respuesta de incidentes; procedimientos para monitoreo, detección, análisis y reportes de eventos e incidentes de seguridad de la información; procedimientos de autenticación para administración de incidentes; procedimientos para manejar evidencia forense; procedimiento para evaluar y decidir acerca de las debilidades de seguridad informática implementada; el personal que manejaría la administración de los incidentes debe estar altamente capacitado para poder hacerlo; referencia formal para procesos disciplinarios para empleados que no cumplan las disposiciones; considerar la retroalimentación oportuna a cada incidente reportado).

Reporte de eventos de seguridad de la información

Requerimiento para Objetivo de Referencia A.16.1.2: Se requiere evidencia de reporte de eventos de seguridad de la información.

Resultado: No hay evidencia. (Se sugiere implementar procedimientos para reportar incidentes o eventos de seguridad de la información

incluyendo escenarios como controles de seguridad ineficientes; brechas de integridad de la información, confidencialidad o disponibilidad; errores humanos; incumplimiento de políticas o directrices; infracciones contra la seguridad física; cambios de aplicaciones no controlados; mal funcionamiento de aplicaciones y equipos; violación de accesos).

Reporte de debilidades de seguridad de la información

Requerimiento para Objetivo de Referencia A.16.1.3: Se requiere evidencia de reporte de debilidades de seguridad de la información.

Resultado: No hay evidencia. (Se recomienda establecer una guía que establezca que todos los empleados y terceros deben reportar dichas novedades tan pronto sea posible con el fin de prevenir incidentes; dicho mecanismo de reporte debe ser fácil, accesible y estar disponible).

Evaluación de eventos de seguridad de la información y decisiones sobre ellos

Requerimiento para Objetivo de Referencia A.16.1.4: Se requiere evidencia de evaluación de eventos de seguridad de la información y decisiones sobre ellos.

Resultado: No hay evidencia. (Se recomienda que se implemente una guía que permita clasificar la escala del incidente; la clasificación y priorización de incidentes puede ayudar a identificar el impacto y alcance de un incidente; considerar que toda resolución debe ser documentada en detalle para futuras referencias).

Respuesta a incidentes de seguridad de la información

Requerimiento para Objetivo de Referencia A.16.1.5: Se requiere evidencia de documentación de respuesta a incidentes de seguridad de la información.

Resultado: No hay evidencia. (Se sugiere que se implemente una guía de respuesta que establezca que la colección de evidencia debe realizarse tan rápido como se pueda; transferir a un análisis forense si el caso lo amerita; escalar el caso si así se lo requiere; asegurar que toda respuesta es documentada para futuro análisis; una vez que el incidente ha sido superado, se debe documentar y cerrar el incidente).

Aprendizaje obtenido de los incidentes de seguridad de la información

Requerimiento para Objetivo de Referencia A.16.1.6: Se requiere evidencia de documentación de aprendizaje en base a los incidentes pasados con respecto a la seguridad de la información.

Resultado: No hay evidencia. (Se sugiere mantener un mecanismo que habilite los tipos, volúmenes y costos de los incidentes de información de seguridad con el fin de mantenerlos cuantificados y monitoreados; la información ganada de la evaluación de los incidentes se la podría utilizar para identificar incidentes recurrentes o de alto impacto).

Recolección de evidencia

Requerimiento para Objetivo de Referencia A.16.1.7: Se requiere evidencia de recolección de evidencia.

Resultado: No hay evidencia. (Se recomienda desarrollar una guía interna para manejar evidencias con fines disciplinarios y que incluya acciones legales; se debe detallar procesos de identificación, colección, adquisición y preservación de las evidencias con diferentes tipos de medio, dispositivos y estados de equipos; debe tomarse en cuenta la cadena de custodia, seguridad de la evidencia, seguridad del personal, roles y responsabilidades del personal involucrado, competencia del personal, documentación e instrucciones).

Protección de registros

Requerimiento para Objetivo de Referencia A.18.1.3: Se requiere documentación que evidencie guías de protección de registros.

Resultado: No conformidad. Existe documentación; sin embargo, no considera procedimientos operacionales y tampoco claves criptográficas. (Se sugiere agregar los siguientes aspectos dentro de la guía, basados en el esquema de clasificación de la organización, los registros deberían ser categorizados en tipo de registros, cada uno con los detalles de periodo de retención y tipo de medio permitido como medio de almacenamiento; cualquier clave criptográfica relacionada y programas asociados con archivos encriptados o firmas digitales debe ser almacenado con el fin de habilitar la desencriptación de los registros por el tiempo que se haya estipulado que estén retenidos).

Privacidad y protección de información de datos personales

Requerimiento para Objetivo de Referencia A.18.1.4: Se requiere evidencia de privacidad y protección de información de datos personales.

Resultado: No conformidad. Se evidencia una carpeta de acceso público con un archivo de extensión MDB, el cual contiene toda la información de los apadrinados. (Se sugiere que la política actual sea implementada y comunicada a todo el personal, la misma requerirá administración apropiada y controlada, debería estar basada en la

legislación relevante y regulaciones pertinentes de protección de privacidad y protección de información personal).

Revisión independiente de la seguridad de la información

Requerimiento para Objetivo de Referencia A.18.2.1: Se requiere evidencia de revisiones de la seguridad de la información.

Resultado: No hay evidencia. (Se recomienda implementar la revisión de la documentación para garantizar la conveniencia, adecuación y eficacia del enfoque de la organización para la gestión de la seguridad de la información; dicha revisión debe incluir la evaluación de oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, los cuales están en los objetivos de la política).

Cumplimiento con las políticas y normas de seguridad

Requerimiento para Objetivo de Referencia A.18.2.2: Se requiere evidencia de cumplimiento de con las políticas y normas de seguridad.

Resultado: No conformidad. El periodo de revisión es muy extendido para los cambios que se han generado en los últimos 6 años. (Se recomienda tener en cuenta la identificación de causas de no cumplimiento; evaluar la necesidad de acciones para alcanzar el cumplimiento de las políticas; implementar acciones correctivas

acertadas; y revisar las acciones correctivas tomadas para verificar su efectividad e identificar cualquier deficiencia o debilidad).

Revisión del cumplimiento técnico

Requerimiento para Objetivo de Referencia A.18.2.3: Se requiere evidencia de revisión del cumplimiento técnico.

Resultado: No hay evidencia. (Se sugiere la realización de la revisión del cumplimiento técnico con herramientas automatizadas, que generen reportes técnicos para su consecuente revisión por un especialista; considerar tener cuidado al utilizar herramientas de penetración o evaluación de vulnerabilidades puesto que dichas actividades pueden conducir a comprometer la seguridad de los sistemas, recordar que éste tipo de pruebas debe ser planificada, documentada y repetida; la revisión del cumplimiento técnico en todo su alcance debe ser realizado por un especialista autorizado o bajo la supervisión del especialista; considerar que la revisión no puede descartar verificar el estado de los sistemas operativos y los equipos).

Una vez terminada la evaluación a cada control de referencia; hay que recalcar cada uno de los resultados fue en su momento conversado con el Gerente de Información y Tecnología con el fin de tener una

explicación más detallada, y así poder determinar si lo evidenciado estaba obteniendo una conclusión acertada.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

Junta de cierre: Celebrada con la participación de Dirección, el Gerente de Información y Tecnología, el Auditor Contable Interno y el auditor autorizado, se procede con la presentación del Informe de Auditoría con el fin de resolver las dudas y controversias del proceso.

3.1. Resultados de auditoría

A continuación se presenta de manera resumida el resultado de la auditoría a la ONG.

Tabla 1 – Tabla de resultados de auditoría por objetivo de control.

Fuente: el autor.

OBJETIVO DE CONTROL		RESULTADO
5.1.1	Políticas para la seguridad de la información.	No conformidad.
5.1.2	Revisión de las políticas para la seguridad de la información.	No conformidad.
6.1.1	Roles y responsabilidades para la seguridad de la información.	No conformidad.
6.1.2	Segregación de responsabilidades.	No conformidad.
6.1.3	Contacto con las autoridades.	No conformidad.
6.2.1	Política para dispositivos móviles.	No conformidad.
6.2.2	Teletrabajo.	No conformidad.
7.1.2	Términos y condiciones del empleo.	Oportunidad de mejora.
7.2.1	Responsabilidades de la dirección.	No conformidad.
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	No conformidad.
8.1.1	Inventario de activos.	No conformidad.
8.1.2	Propiedad de los activos.	No conformidad.
8.1.3	Uso aceptable de los activos.	No conformidad.
8.1.4	Devolución de activos.	No conformidad.
8.2.1	Clasificación de la información	No hay evidencia.
8.2.2	Etiquetado de la información.	No hay evidencia.
8.2.3	Manejo de activos.	No conformidad.
8.3.1	Gestión de medios removibles.	No conformidad.
8.3.2	Eliminación de los medios.	No conformidad.
8.3.3	Transferencia de medios físicos.	No hay evidencia.
9.1.1	Política de control de acceso	No conformidad.
9.1.2	Acceso a redes y a servicios en red.	Oportunidad de mejora.
9.2.1	Registro y cancelación del registro de	No hay evidencia.

	usuarios.	
9.2.2	Suministro de acceso de usuarios.	No hay evidencia.
9.2.3	Gestión de derechos de acceso privilegiado.	No hay evidencia.
9.2.4	Gestión de información de autenticación secreta de usuarios.	No hay evidencia.
9.2.5	Revisión de los derechos de acceso de usuarios.	No hay evidencia.
9.2.6	Retiro o ajuste de los derechos de acceso.	No hay evidencia.
9.3.1	Uso de información de autenticación secreta.	No hay evidencia.
9.4.1	Restricción de acceso a la información.	No hay evidencia.
9.4.2	Procedimiento de ingreso seguro.	No conformidad.
9.4.3	Sistema de gestión de contraseñas.	No conformidad.
9.4.4	Uso de programas de utilidad privilegiados.	No hay evidencia.
9.4.5	Control de acceso a código fuente de aplicativos.	No conformidad.
10.1.1	Política sobre uso de controles criptográficos.	No hay evidencia.
10.1.2	Administración de llaves.	No hay evidencia.
11.1.1	Perímetro de seguridad.	No conformidad.
11.1.2	Controles de acceso físicos.	No conformidad.
11.1.3	Seguridad de oficinas, recintos e instalaciones.	No conformidad.
11.1.4	Protección contra amenazas externas y ambientales.	Oportunidad de mejora.
11.1.5	Trabajo en áreas seguras.	Oportunidad de mejora.
11.1.6	Áreas de despacho y carga.	No conformidad.
11.2.1	Ubicación y protección de los equipos.	No conformidad.
11.2.3	Seguridad del cableado.	Oportunidad de mejora.
11.2.4	Mantenimiento de equipos.	Oportunidad de mejora.
11.2.5	Retiro de activos.	Oportunidad de mejora.
11.2.6	Seguridad de equipos y activos fuera de las instalaciones.	No conformidad.
11.2.7	Eliminación segura o reutilización de equipos.	No conformidad.
11.2.8	Equipos de usuario desatendido.	No hay evidencia.
11.2.9	Política de escritorio limpio y pantalla limpia.	No hay evidencia.
12.1.1	Procedimientos de operación documentados.	No conformidad.

12.1.2	Gestión de cambios.	No hay evidencia.
12.1.4	Separación de los ambientes de desarrollo, pruebas, y operaciones.	No hay evidencia.
12.2.1	Controles contra códigos maliciosos.	No conformidad.
12.5.1	Instalación de aplicativos en sistemas operativos.	Oportunidad de mejora.
12.6.1	Gestión de las vulnerabilidades técnicas.	No conformidad.
12.6.2	Restricciones sobre la instalación de aplicativos.	Oportunidad de mejora.
13.1.1	Controles de red.	No conformidad.
13.1.2	Seguridad de los servicios de red.	Oportunidad de mejora.
13.1.3	Separación en las redes.	Oportunidad de mejora.
13.2.3	Mensajería electrónica.	No conformidad.
13.2.4	Acuerdos de confidencialidad o de no divulgación.	No conformidad.
16.1.1	Responsabilidades y procedimientos.	No hay evidencia.
16.1.2	Reporte de eventos de seguridad de la información.	No hay evidencia.
16.1.3	Reporte de debilidades de seguridad de la información.	No hay evidencia.
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	No hay evidencia.
16.1.5	Respuesta a incidentes de seguridad de la información.	No hay evidencia.
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.	No hay evidencia.
16.1.7	Recolección de evidencia.	No hay evidencia.
18.1.3	Protección de registros.	No conformidad.
18.1.4	Privacidad y protección de información de datos personales.	No conformidad.
18.2.1	Revisión independiente de la seguridad de la información.	No hay evidencia.
18.2.2	Cumplimiento con las políticas y normas de seguridad.	No conformidad.
18.2.3	Revisión del cumplimiento técnico.	No hay evidencia.

La Tabla 1, resultados de auditoría por objetivo de control, muestra en resumen, la conclusión obtenida luego de haber evaluado cada uno de

los controles de referencia asociados a los objetivos de control. Para una mejor visualización del resultado de la auditoría se generó la siguiente gráfica:

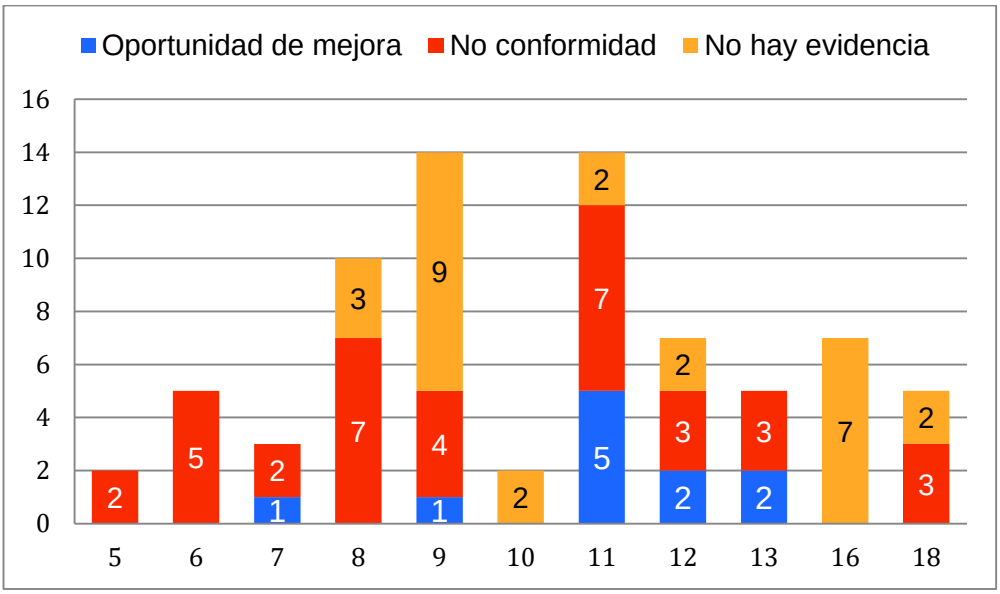


Figura 3.1 – Gráfica de Objetivos de Control Vs. Cantidad de controles auditados. Fuente: el autor.

La Figura 3.1 muestra la cantidad de controles que se auditaron por objetivo de control, indicando por color el nivel de la implementación del control, siendo el color rojo el designado para las no conformidades, el naranja para aquellos controles que no se pudieron evidenciar, y azul para los controles que tienen una oportunidad de mejora.

A partir de la gráfica podemos decir lo siguiente:

- No existe objetivo de control que esté bien implementado y controlado dentro de la organización,
- Los objetivos de control 5 – Políticas de la Seguridad de la Información, 7 – Seguridad de los Recursos Humanos, 8 – Gestión de activos, 9 – Control de acceso, 10 – Criptografía, 11 – Seguridad física y del entorno, 12 – Seguridad de las operaciones, y 13 – Seguridad de las comunicaciones, considerados como de mayor impacto para el fin de la auditoría, mantienen un alto número de no conformidades (exceptuando el objetivo de control 10, el cual no se pudo evidenciar), por lo que se tendrá que implementar una gran cantidad de cambios para poder conseguir una cultura organizacional de seguridad de la información en un futuro, y
- Teniendo en cuenta que todos los objetivos de control son importantes, habría que iniciar con un plan de acción inmediato en los objetivos 5 – Políticas de la Seguridad de la Información, 6 – Organización de la Seguridad de la Información, 7 – Seguridad de los Recursos Humanos, 8 – Gestión de activos, 11 – Seguridad física y del entorno, 13 – Seguridad de las comunicaciones, y 18 – Cumplimiento, objetivos de control que

mantienen un número mayor de controles con no conformidad evaluada.

Veamos desde una perspectiva general, el resultado de la auditoría a través del siguiente gráfico:

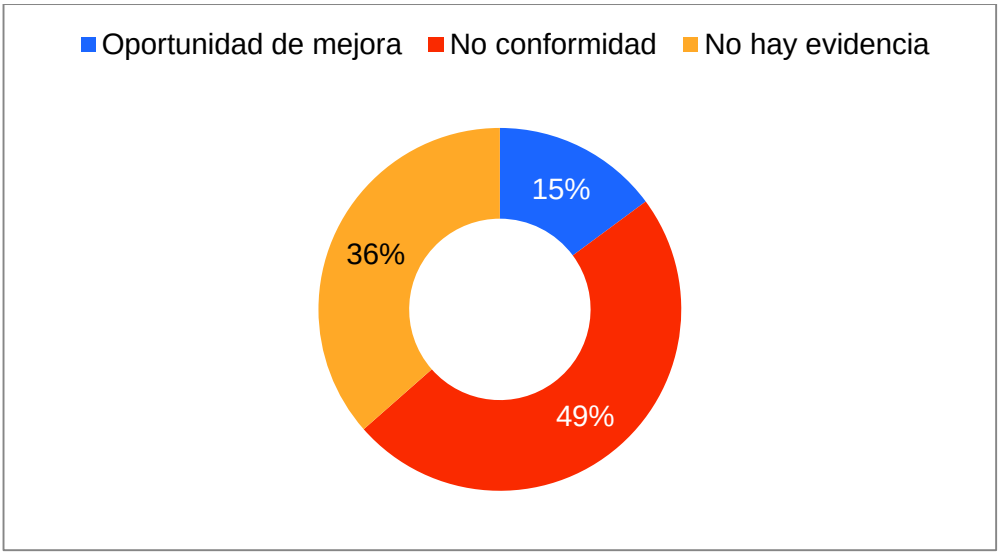


Figura 3.2 – Gráfica porcentual de resultados. *Fuente: el autor.*

Tal como se puede ver en la Figura 3.2, el estado de la ONG no es muy favorable; el 49% de los controles auditados presentan un estado de no conformidad; un 36% corresponde a aquellos que no se pudieron evidenciar y apenas un 15% de los controles auditados tienen una oportunidad de mejora.

3.2. Plan de resolución de no conformidades y oportunidades de mejora

El cliente acepta las recomendaciones en el caso de las no conformidades y oportunidades de mejora, a continuación descritas por cada control de referencia:

A.5.1.1: Se sugiere definir una Política de Seguridad de la Información, que sea aprobada por administración y que considere aspectos como la estrategia del negocio; regulaciones, contratos y legislación; objetivos y principios que sirva de guía para todas las actividades relacionadas a seguridad de la información; procesos de manejo de excepciones.

A.5.1.2: Se recomienda que la política definida esté a cargo de una persona, la cual será responsable del desarrollo, revisión y evaluación de las políticas. Tomar en cuenta que las revisiones que se realicen deben incluir evaluaciones de oportunidades para mejorar las mismas y alcanzar los objetivos establecidos.

A.6.1.1: Se sugiere que la responsabilidad sobre los recursos y la implementación de los controles caiga sobre cada empleado, protegiendo día a día cada uno de sus activos a cargo.

A.6.1.2: Se recomienda tomar en cuenta el control como un método de reducir el riesgo accidental o mal uso deliberado de un activo de la organización.

A.6.1.3: Se sugiere mantener una documentación apropiada de contactos, sería de gran ayuda como soporte a la continuidad del negocio y los planes de contingencia.

A.6.2.1: Se recomienda tener por separado el uso de dispositivos móviles para uso personal y laboral, incluyendo aplicativos que ayuden a dicha segmentación con el fin de proteger los datos de la organización en el dispositivo privado. El acceso a la información laboral a través de dispositivos móviles debe darse únicamente luego de haber firmado un acuerdo de conocimiento de responsabilidades, las cuales incluyen protección física y actualización de aplicativos, renunciando a ser propietario de los datos de la empresa, permitiendo limpieza remota de datos en caso de robo, pérdida del dispositivo, o desautorización del uso del mismo. Tener en cuenta que la información almacenada en dispositivos móviles podrían no ser respaldados bajo el escenario de limitaciones de ancho de banda en la

red o porque el dispositivo puede no estar encendido en los horarios establecidos para respaldos.

A.6.2.2: Se sugiere provisionar equipos debidamente configurados y dispositivos de almacenamiento para actividades de teletrabajo, en donde se garantice que equipos no autorizados no puedan conectarse a los aplicativos de la organización; la información a la que tenga acceso deberá estar debidamente clasificada y protegida; acceso remoto seguro debería ser provisionado; seguridad física; procesos de respaldo y continuidad de negocio; y monitoreo continuo de seguridad.

A.7.1.2: Se recomienda asegurarse que tanto los empleados como los terceros, estén de acuerdo con los términos y condiciones que contempla la seguridad de la información.

A.7.2.1: Se recomienda tener en cuenta que el no tener los roles y responsabilidades definidas, puede causar considerable daño a la organización. Recordar que si el personal está motivado se puede obtener un comportamiento laboral que cause menos incidentes en cuanto a seguridad de la información.

A.7.2.2: Se sugiere tener en cuenta que el entrenamiento puede realizarse en una sala de clase, a distancia, basado en web, autoaprendizaje y otros; el detalle está en que se cubran temas como el compromiso de todos con respecto a la seguridad de la información; la necesidad de familiarizarse con las reglas y obligaciones de la seguridad de la información definidas en políticas, estándares, leyes, regulaciones, contratos y acuerdos; responsabilidad por las acciones e inacciones tomadas en cuando a protección de la información, incluyendo el monitoreo hacia terceras personas; plan de comunicación de incidentes y conceptos generales de procedimientos de seguridad, como por ejemplo la seguridad de las contraseñas, malware y escritorios limpios; puntos de información en dónde se pueda consultar nuevas formas o mecanismos de protección con el fin de mejorar continuamente los conocimientos ya adquiridos.

A.8.1.1: Se recomienda considerar que el documento que detalla el ciclo de vida de información debe incluir desde la creación, el procesamiento, el almacenamiento, la transmisión, la eliminación y la destrucción; éste debe estar debidamente actualizado, ser consistente y registrar siempre el responsable.

A.8.1.2: Se sugiere tener presente que el responsable debe asegurar que el activo esté inventariado; asegurar que el activo esté debidamente clasificado y protegido; definir y periódicamente revisar las restricciones de acceso y clasificación de los activos más importantes teniendo en cuenta las políticas de control de acceso definidas; y asegurar apropiado manejo cuando el activo es eliminado o destruido.

A.8.1.3: Se recomienda que empleados y terceros que tengan acceso a la organización sean concientizados sobre las políticas de seguridad de la información, responsabilizándolos por su uso durante el tiempo que estén vinculados a la organización.

A.8.1.4: Se sugiere considerar que la terminación del proceso debería ser formalizada una vez se hayan recibido todos los activos de información y electrónicos que la organización otorgó en su momento al empleado o terceros. Si se ha utilizado equipos personales, la información que se maneje en estos equipos deberá ser transferida al término de la actividad. Durante el periodo de terminación la organización debe tener control sobre la copia no autorizada de información relevante de la organización.

A.8.2.3: Se sugiere incluir las restricciones de acceso para el apoyo de requerimientos de protección por cada nivel de clasificación; protección de copias de información, temporal o permanente, a un nivel consistente con la protección de información original; almacenamiento de activos de TI en acuerdo con las especificaciones de fábrica; marcado claro de todas las copias de medios para la atención del recipiente autorizado.

A.8.3.1: Se sugiere reforzar el procedimiento con guías para asegurar que medios removibles no requeridos, deben de estar bajo un proceso de borrado de información no recuperable; en caso de ser necesario y práctico, la autorización debe ser requerida para la eliminación de los mismos dejando un registro de dichos medios para efectos de auditoría; todos los medios removibles deberían ser almacenados en un lugar seguro bajo las especificaciones de fábrica; en caso de ser necesario por efectos de confidencialidad o integridad en algunos datos, se debería utilizar técnicas de criptografía para proteger los datos en medios removibles; para evitar el riesgo de daño mientras la información es aún necesaria, la data debería ser transferida a un medio extraíble nuevo antes de que se vuelva difícil de leer en el anterior, todo esto debidamente monitoreado; en caso de datos importantes se debería tener múltiples copias y almacenarlas en

medios separados y apartados con el fin de reducir el riesgo de pérdida o daño de datos; registro de medios removibles deberían ser mantenidos para limitar posibles pérdidas de datos; tener en consideración que los medios removibles únicamente deben ser habilitados si existe alguna razón justificada para hacerlo.

A.8.3.2: Se sugiere modificar la guía y agregar mayor detalle acerca del manejo de medios con información confidencial a ser eliminados, manteniéndolos en un lugar seguro y eliminándolos de forma segura; se debería clasificar aquellos medios que tengan información sensible para una rápida identificación y una segura eliminación; si se dispone de algún servicio de retiro y eliminación de medios, se debe tener cuidado en la selección del tercero, el cual debe tener experiencia verificable en la ejecución de lo requerido; todo medio a ser eliminado debería ser registrado para efectos de auditoría; se debe tener presente que todo medio dañado que contenga datos sensibles deben ser sometidos a decisión para ver si es mejor arreglarlos antes que eliminarlos.

A.9.1.1: Se sugiere se tome en cuenta aspectos como políticas de diseminación y autorización; consistencia entre los derechos de acceso y la clasificación de información tanto en aplicativos como red

interna; legislación relevante y cualquier obligación contractual establecida que requiera acceso a datos o servicios; administración de derechos de acceso en un ambiente distribuido y conectado que reconozca todos los tipos de conexiones disponibles; segregación de roles en cuanto a control de acceso; requerimientos formales para solicitar acceso; proceso de revisión de la política de derechos de acceso y retiro de los mismos; registro de eventos significativos concernientes al uso y administración de identidades de usuarios e información de autenticación.

A.9.1.2: Se sugiere tener en cuenta algún mecanismo propio que les permita monitorear el uso de los servicios de red.

A.9.4.2: Se recomienda agregar una técnica de autenticación acorde que involucre verificación de identidad de usuario, algunos ejemplos son métodos criptográficos, tarjetas inteligentes, *tokens* o biométricos. Tener en cuenta que el procedimiento de autenticación a un sistema o aplicativo debe ser diseñado para minimizar la oportunidad a que usuarios no autorizados tengan acceso, algunos aspectos a considerar pueden ser el no mostrar evidencia alguna de anteriores usuarios autenticados; no mostrar información parcial hasta que se haya completado el proceso como tal; mostrar un mensaje general de

que el computador debe ser accedido únicamente por usuarios autorizados; ante cualquier fallo de autenticación el sistema no debe indicar que parte en específico fue la que ocasionó el fallo; mantener protección en contra de mecanismos como fuerza bruta; mantener un historial de autenticaciones exitosas y no exitosas; levantar un evento de seguridad si se identifica un comportamiento comprometido en el proceso de autenticación; se debe mostrar para el escenario de autenticación exitosa datos como fecha y hora de la última conexión y detalles de cualquier autenticación no exitosa desde la última conexión exitosa realizada; tener en cuenta que jamás se debería mostrar la contraseña en el campo respectivo; considerar no permitir la transmisión de contraseñas en texto plano sobre la red; cerrar sesiones inactivas luego de un tiempo prudencial; y definir horario de conexiones restringidas con el fin de disminuir el alto riesgo por conexiones no autorizadas.

A.9.4.3: Se sugiere tomar en consideración aspectos como el refuerzo de que el uso de los identificadores y las claves son personales; permitir al usuario seleccionar y cambiar sus propias contraseñas e incluir una confirmación de culminación de procedimiento; no mostrar la contraseña en la pantalla; guardar los archivos de contraseñas lejos del lugar en donde se encuentren los datos; la transmisión y

almacenamiento de las contraseñas se debe realizar de manera segura; reforzar la selección de claves de calidad; y considerar mantener un registro de contraseñas utilizadas para prevenir el reúso de las mismas.

A.9.4.5: Se sugiere elevar los controles de restricción teniendo en cuenta los siguientes aspectos, donde sea posible, las librerías fuentes de los programas no deben estar almacenados en los sistemas operativos; el código fuente y las librerías deben ser administradas acorde a procedimientos establecidos; el personal de soporte no debe tener acceso no restringido al código fuente o librerías; las actualizaciones de los programas deben realizarse una vez se tenga la autorización correspondiente; considerar que el historial de accesos a los códigos fuentes y librerías debe ser realizado; el mantenimiento y copia del código fuente debe ser sujeto a procedimientos de control de cambios estrictos.

A.11.1.1: Se sugiere el desarrollo de una política de seguridad perimetral definida y usada para proteger áreas que contengan información crítica o sensible, teniendo en cuenta que barreras físicas, en donde aplique, deben ser construidas para prevenir acceso físico no autorizado y contaminación del área por el ambiente; todas las

puertas de salida en caso de incendio deberán tener alarma en caso de encontrarse dentro del perímetro de seguridad, considerar que deben ser monitoreadas y probadas; sistemas de detección de intrusos deben ser incorporados para complementar la seguridad; las instalaciones físicas del procesamiento de información debe estar separado de aquellos espacios administrados por terceras personas.

A.11.1.2: Se sugiere tener en cuenta los siguientes aspectos en la documentación actual, la fecha y hora de entrada y salida de visitantes debe ser supervisada y registrada; el acceso a las áreas en donde información confidencial es procesada o almacenada debe ser restringida a personal no autorizado; todo empleado o tercera persona debe vestir una identificación visible que permita llevar un control sobre individuos que estén dentro del perímetro restringido; toda tercera persona debe tener autorización para poder ingresar al área restringida; la política debe ser revisada con regularidad y actualizada cuando sea necesario.

A.11.1.3: Se recomienda tener en cuenta dentro de la política que las instalaciones claves deberían estar situadas estratégicamente para evitar el acceso de personal no autorizado; donde sea aplicable, se deberá establecer el entorno de tal forma que actividades que

involucren información confidencial no puedan ser ni visualizadas ni escuchadas por terceros; el directorio y los libros telefónicos internos que identifican localidades de procesamiento de información confidencial no deben ser de fácil acceso para la lectura de personal no autorizado.

A.11.1.4: Se sugiere pedir ayuda a un profesional en cómo evitar daños causados por fuego e inundaciones.

A.11.1.5: Se recomienda tomar en consideración evitar el trabajo no supervisado en áreas seguras por razones de seguridad y para prevenir oportunidades para la ejecución de actividades maliciosas.

A.11.1.6: Se sugiere tomar en consideración los siguientes aspectos, el acceso al área de carga y despacho debe estar fuera del inmueble principal y con acceso restringido; el área de carga y despacho debe estar diseñada para que personal no autorizado entre en el edificio; todo material que ingrese debe ser registrado en acuerdo con los procedimientos de administración de activos e inspeccionado.

A.11.2.1: Se recomienda tomar en cuenta aspectos como situar los equipos de tal modo que se reduzca el acceso innecesario al área de

trabajo por terceros, permitiéndoles visualizar información que puede ser categorizada como sensible; adoptar controles para reducir el riesgo de problemas potenciales de tipos físico y ambiental; guías para comer, beber, y/o fumar deben ser establecidas bajo escenarios de proximidad con instalaciones de procesamiento de información; las condiciones ambientales, como la temperatura y la humedad deben ser monitoreadas por condiciones que afecten las operaciones de procesamiento de información.

A.11.2.3: Se sugiere controlar el acceso al área de *patch panels* y cuarto de cables.

A.11.2.4: Se recomienda considerar aspectos como las especificaciones de equipos para coordinar la frecuencia del mantenimiento; recordar que sólo el personal autorizado debe llevar a cabo las reparaciones y mantenimientos; se debe llevar una bitácora por equipo en cuanto a mantenimientos preventivos y correctivos; controles apropiados deben ser tomados en cuenta al momento de la ejecución del mantenimiento, en especial si el servicio lo otorga un tercero; antes de devolver el equipo a su lugar asignado, debe ser chequeado con el fin de verificar que no haya sido dañado o intervenido.

A.11.2.5: Se recomienda tener en cuenta un límite de tiempo para remover activos y la verificación de los mismos al cumplirse el mantenimiento.

A.11.2.6: Se recomienda que se tenga en consideración que el uso de cualquier dispositivo de almacenamiento de información y equipos fuera de la organización debe ser autorizado por la directora; esto aplicaría también a equipos propios que son utilizados para la organización; considerar el hecho de que no se deben dejar en desatención en ningún momento; en caso de que el equipo sea transferido mientras se encuentre fuera de la organización, se debe llevar una cadena de custodia que detalle el propietario temporal y la organización responsable.

A.11.2.7: Se recomienda que los equipos sean verificados para asegurar que los medios de almacenamiento se destinen a su eliminación o a su reúso; tener en cuenta mecanismos de borrado antes de su eliminación o reúso por parte de terceros.

A.12.1.1: Se recomienda que la documentación de los procedimientos esté desarrollada para actividades operacionales alineadas con el procesamiento de información e instalaciones de comunicaciones;

incluyendo la instalación y configuración de aplicativos; procesamiento y manejo de información de manera automática y manual; respaldos; requerimientos agendados, incluyendo interdependencias entre sistemas internos y externos; considerar las instrucciones para manejo de errores u otras condiciones excepcionales que puedan presentarse durante la ejecución de algún *job*; soporte y contacto de respaldo incluyendo el soporte efectuado por terceros; instrucciones de manejo de medios y resultados especiales, incluyendo eliminación segura de resultados de un *job* fallido; contemplar procedimientos de reinicio y recuperación para el uso de eventos de falla del sistema; la administración de historial de log; monitoreo continuo de procedimientos.

A.12.2.1: Se recomienda que se tome a consideración el hecho de que la protección contra el malware debe estar basada en detección de malware y reparación de aplicativos, advertencia de seguridad de la información y acceso apropiado a los sistemas, y control de gestión de cambios. La política debería incluir un procedimiento formal que prohíba el uso de aplicativos no autorizados; la implementación de controles que prevengan o detecten el uso de aplicaciones no autorizadas; la implementación de controles que prevengan o detecten el uso de sitios de Internet no recomendables; protección contra

riesgos asociados con la recepción de archivos y aplicativos, ya sea vía externa o cualquier medio; administración técnica de vulnerabilidades; instalación y actualización regular de detección de malware para escanear computadores y medios como medida de precaución; preparación del plan de continuidad en caso de presentarse un ataque producido por un malware; aislar ambientes donde se pueda ser víctima de un resultado catastrófico.

A.12.5.1: Se sugiere tener en cuenta los siguientes aspectos, la actualización de los aplicativos y librerías de programas deben ser realizadas por administradores entrenados previamente autorizados; los controles de configuración de los sistemas deben ser utilizados para mantener el control de todos los aplicativos implementados así como la documentación de cada uno; considerar mantener un log para auditorías, el mismo debe contemplar todas las actualizaciones aplicadas; la versión inmediata anterior debe ser mantenida como medida de contingencia.

A.12.6.1: Se recomienda que se realice un inventario de activos completo como prerrequisito para la administración técnica efectiva de vulnerabilidades. Tomar en cuenta que las acciones apropiadas deben ser tomadas a tiempo en respuesta a la identificación de

vulnerabilidades potenciales; la organización debe definir y establecer roles y responsabilidades asociadas con administración de vulnerabilidades, incluyendo el monitoreo, evaluación de riesgo, parche, seguimiento y cualquier otra responsabilidad requerida de coordinación; una vez detectada la vulnerabilidad, la organización debe identificar los riesgos asociados y las acciones a ser tomadas; el riesgo de instalar parches debe ser evaluado antes de cualquier aplicación; considerar que los sistemas con gran riesgo deben ser atendidos primero.

A.12.6.2: Se sugiere que la organización mejore y haga cumplir la política sobre qué tipos de aplicativos pueden ser instalados por usuarios; la instalación no controlada de aplicativos puede acarrear grandes consecuencias como la introducción de posibles vulnerabilidades, pérdida de la integridad de la información u otros incidentes de la seguridad de la información.

A.13.1.1: Se sugiere que se incrementen controles para asegurar la seguridad de la información en redes y la protección de servicios conectados de accesos no autorizados; la administración de los equipos de redes deben ser documentados bajo procedimientos de responsabilidades; las responsabilidades operacionales en redes

deben estar separadas de las operaciones del computador; controles especiales deben de establecerse para salvaguardar la confidencialidad e integridad de los datos que pasan por las redes públicas; registros de log y monitoreo continuo deberían ser habilitados con el fin de detectar acciones que puedan afectar la seguridad de la información; sistemas utilizados sobre la red deberían de contar con autenticación; contemplar que la conexión a la red sea restringida.

A.13.1.2: Se recomienda que siempre se supervise y determine la capacidad del proveedor del servicio de red para gestionar los servicios acordados; es necesario la identificación de medidas de seguridad necesarias para determinados servicios, tales como características de seguridad, niveles de servicio y requisitos de gestión; implementar soluciones como firewalls y sistemas de detección de intrusos.

A.13.1.3: Se sugiere que en caso de activar las redes inalámbricas recuerden darle un tratamiento especial debido al pobre perímetro de red definido.

A.13.2.3: Se recomienda que se considere protección de mensajes de accesos no autorizados, modificaciones o denegación de servicio; asegurar correcto direccionamiento y transportación del mensaje; confiabilidad y disponibilidad de servicio; consideraciones legales para el caso de firmas electrónicas; aprobación previa antes de usar servicios públicos externos como mensajería instantánea, redes sociales o compartición de archivos; fuertes niveles de autenticación de redes públicas.

A.13.2.4: Se sugiere que se mejoren los acuerdos de confidencialidad o no divulgación con el fin de proteger la información usando términos de referencia legal; estos acuerdos deben ser aplicados a terceros y empleados de la organización.

A.18.1.3: Se sugiere agregar los siguientes aspectos dentro de la guía, basados en el esquema de clasificación de la organización, los registros deberían ser categorizados en tipo de registros, cada uno con los detalles de periodo de retención y tipo de medio permitido como medio de almacenamiento; cualquier clave criptográfica relacionada y programas asociados con archivos encriptados o firmas digitales debe ser almacenado con el fin de habilitar la desencriptación

de los registros por el tiempo que se haya estipulado que estén retenidos.

A.18.1.4: Se sugiere que la política actual sea implementada y comunicada a todo el personal, la misma requerirá administración apropiada y controlada, debería estar basada en la legislación relevante y regulaciones pertinentes de protección de privacidad y protección de información personal.

A.18.2.2: Se recomienda tener en cuenta la identificación de causas de no cumplimiento; evaluar la necesidad de acciones para alcanzar el cumplimiento de las políticas; implementar acciones correctivas acertadas; y revisar las acciones correctivas tomadas para verificar su efectividad e identificar cualquier deficiencia o debilidad.

El cliente se compromete a establecer las actividades para elaborar, actualizar y realizar seguimiento a los planes de resolución de no conformidades y oportunidades de mejora, con el fin de determinar las acciones preventivas, correctivas y de mejora de conformidad con los hallazgos identificados.

CONCLUSIONES Y RECOMENDACIONES

Al concluir el presente trabajo de auditoría, se puede mencionar lo siguiente en cuanto a conclusiones:

1. La mayoría de las operaciones de las áreas funcionales no son lo suficientemente eficientes, se mantiene una gran cantidad de controles de referencia sin la correcta implementación;
2. La comunicación entre departamentos es crucial si se requiere coherencia entre las normas departamentales que al final ayudarán al cumplimiento de la visión y misión de la organización;

3. Se determinaron 36 vulnerabilidades directas de seguridad de la información y 27 vulnerabilidades de nivel bajo, de un total de 74 controles de referencia auditados.

Adicionalmente se contemplan las siguientes recomendaciones:

1. Capacitar al personal en base a las políticas existentes y futuras. Se pueden adoptar distintos mecanismos de defensa para contrarrestar las vulnerabilidades encontradas; sin embargo, todos ellos resultarán inútiles si el capital humano no se encuentra debidamente capacitado y con el criterio acertado para actuar bajo las actividades que se realizan de manera diaria;
2. Realizar al menos dos auditorías al año con el fin de verificar que las mejoras implementadas estén cumpliendo su objetivo, y constatar la existencia o no de nuevas vulnerabilidades;
3. Implementar el Plan de Resolución de no conformidades y oportunidades de mejora con el fin de ayudar a mitigar el malware, la ingeniería social y la violación de contraseñas dentro de la organización.

BIBLIOGRAFÍA

[1] ISO/IEC 27002:2013, Information Technology. *Security techniques. Code of Practice for Information Security Control*.

[2] Karina, A. B. (2013). Hacking Ético 101, *Cómo hackear profesionalmente en 21 días o menos!*

[3] ISO/IEC 27001, Information technology. Security techniques. Information security management systems - Requirements.

[4] http://www.iso.org/iso/home/standards.htm, 2016.

[5] Abraham, Nyirongo. (2015). Auditing Information Systems, *Performance of the Enterprise*.

ANEXOS

Anexo 1 - Objetivos de Control y Controles de Referencia. **Fuente: basado en ISO/IEC27002:2013 [1]**

A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN		
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información		
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	Control: se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su continua conveniencia, adecuación y eficacia.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1 Organización Interna		
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la		

organización.		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.
A.6.2 Dispositivos móviles y teletrabajo		
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles		
A.6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS		
A.7.1 Antes de asumir el empleo		
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		
A.7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.

A.7.2 Durante la ejecución del empleo		
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan		
A.7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
A.8 GESTIÓN DE ACTIVOS		
A.8.1 Responsabilidad por los activos		
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		
A.8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.
A.8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su

		empleo, contrato o acuerdo.
A.8.2 Clasificación de la información		
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización		
A.8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3 Manejo de medios		
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios.		
A.8.3.1	Gestión de medios removibles	Control: Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios	Control: Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

A.9 CONTROL DE ACCESO		
A.9.1 Requisitos del negocio para control de acceso		
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información		
A.9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Acceso a redes y a servicios en red	Control: Sólo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2 Gestión de acceso de usuarios		
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios		
A.9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.

A.9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
A.9.3 Responsabilidades de los usuarios		
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación		
A.9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4 Control de acceso a sistemas y aplicaciones		
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones		
A.9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
A.9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a código fuente de	Control: Se debe restringir el acceso al código fuente de los aplicativos.

	aplicativos	
A.10 CRIPTOGRAFÍA		
A.10.1 Controles criptográficos		
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información		
A.10.1.1	Política sobre uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Administración de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO		
A.11.1 Áreas seguras		
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización		
A.11.1.1	Perímetro de seguridad	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
A.11.1.2	Controles de acceso físicos	Control: Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales	Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas	Control: Se deben diseñar y aplicar

	seguras	procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga	Control: Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2 Equipos		
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
A.11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
A.11.2.3	Seguridad del cableado	Control: El cableado de energía eléctrica y de comunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos	Control: Los equipos, información o aplicativos no se deben retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o aplicativo licenciado haya sido retirado o sobrescrito en forma segura antes de

		su disposición o reúso.
A.11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da la protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12 SEGURIDAD DE LAS OPERACIONES		
A.12.1 Procedimientos operacionales y responsabilidades		
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información		
A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
A.12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operaciones	Control: Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2 Protección contra códigos maliciosos		
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		
A.12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos

		maliciosos.
A.12.5 Control de aplicativo operacional		
Objetivo: Asegurarse de la integridad de los sistemas operacionales		
A.12.5.1	Instalación de aplicativos en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de aplicativos en sistemas operativos.
A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de aplicativos	Control: Se debe establecer e implementar las reglas para la instalación de aplicativos por parte de los usuarios.
A.13 SEGURIDAD DE LAS COMUNICACIONES		
A.13.1 Gestión de la seguridad de las redes		
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte		
A.13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten

		internamente o se contraten externamente.
A.13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A.13.2 Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.3	Mensajería electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información		
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades		
A.16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la	Control: Se debe exigir a todos los empleados y contratistas que usan los

	información	servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.18 CUMPLIMIENTO		
A.18.1 Cumplimiento de requisitos legales y contractuales		
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad		
A.18.1.3	Protección de registros	Control: Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la

		reglamentación pertinentes, cuando sea aplicable.
A.18.2 Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales		
A.18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.