Universidad CENFOTEC

Maestría en Ciber Seguridad

Documento final de Proyecto de Investigación Aplicada 2

Tema:

Implementación de las bases para la seguridad de la información apoyada en tecnologías de código abierto para Edificadora Beta.

Estudiante:

Buján Ugalde, Roberto Ricardo

Fecha: julio, 2017

Dedicatoria

A Dios por darme la vida, salud y sabiduría para afrontar obstáculos en el camino. A mis padres por formarme con amor y cariño. A mi esposa Adriana y a mi hija Valeria, por demostrarme día con día el significado de la valentía y el esfuerzo de luchar por un objetivo, trabajar duro y conseguirlo.

Agradecimientos

En primera instancia agradezco profundamente al profesor Luis Carlos Naranjo, por el apoyo en el desarrollo del presente trabajo de graduación, por la orientación brindada y el seguimiento al logro de los objetivos planteados mediante sus recomendaciones.

Igualmente, correspondo mi gratitud al Sr. Manrique Rojas y al Sr Eduardo Mora, por permitirme y ayudarme a desarrollar este proyecto en la edificadora Beta, por facilitar la información requerida, el desarrollo de los temas de este proyecto y a la vez por los comentarios emitidos durante la elaboración de este.

Resumen

La motivación para este proyecto nace ante el enfoque de modelo de mantenimiento de las tecnologías de la información (TI) en empresas pequeñas, el cual está basado en un modelo de “si funciona, no lo toque”, en donde lo que se persigue es que los sistemas de información estén disponibles y por tanto, no se le da tanta importancia a la confidencialidad, ni a la integridad de la información por diversos factores. El problema de este enfoque, ampliamente difundido en Costa Rica, consiste en que ya no solo las empresas extranjeras multimillonarias son blancos de ataques en su seguridad de la información, sino que cada día más y más empresas medianas y pequeñas son víctimas del hampa, lo que causa pérdidas cuantiosas que pudieron evitarse si hubieran existido una adecuada cultura de seguridad en el manejo de la información.

El presente proyecto pretendió crear una propuesta e implementación de un esquema de seguridad de la información para una pequeña empresa, la edificadora Beta, quienes recién se han concientizado sobre la necesidad de proteger su información no solo de la no disponibilidad, sino también a los accesos no autorizados y corrupción de estos. Para lograrlo se utilizaron las mejores prácticas de seguridad establecidas por la industria, tecnologías existentes en la empresa, así como herramientas de código abierto como apoyo. Esto dio como resultado controles de seguridad para un manejo de la información valiosa de la empresa de manera mucho más robusta.

Carta de aceptación

San Carlos, 22 de junio del 2017

Carta de intención para la propuesta y ejecución del proyecto de "*Implementación de las bases de infraestructura de red apoyada en tecnologías de código abierto para Edificadora Beta*" para el año 2017, que celebran por una parte el Sr. Manrique Rojas, gerente general de la empresa Edificadora Beta, y el Sr. Roberto Buján Ugalde, aspirante al grado de Maestría en Ciber Seguridad de la Universidad CENFOTEC_

Tema: Implementación de las bases de infraestructura de red apoyada en tecnologías de código abierto para Edificadora Beta

Objetivos: Diseñar una propuesta para asegurar la infraestructura de red de la Edificadora Beta, así como la implementación parcial de los controles resultantes sugeridos en dicho análisis.

Alcances: Se establece como el alcance la creación de la propuesta de aseguramiento de la información basado en un análisis profundo de la situación actual de la empresa, así como la implementación de los controles que sean viables, como también los pasos a seguir para implementar más adelante el resto de los controles cuando se cuente con los prerrequisitos para llevarlos a cabo.

Limitaciones: Parte de las limitantes que de identifican son:

- Factor económico: La propuesta pretende sugerir controles alternativos a los comerciales para disminuir el costo de estos, ya que dichas versiones comerciales suelen ser costosas.
- Factor Tiempo: Para implementar muchas de las mejoras, se requiere la inversión de tiempo, para llegar a implementar las propuestas, como, por ejemplo, la elaboración de planes de entrenamiento para el personal, así como impartir dichos entrenamientos.

Requisitos:

- Apoyo y compromiso por parte de la gerencia a la hora de facilitar la información y considerar las propuestas para implementarlas en el momento que ellos consideren más oportuno.

Manrique Rojas.

Roberto Buján

Tabla de contenidos

Figuras

Tablas

Capítulo 1: Introducción

Durante el desarrollo de este proyecto se buscó evaluar la condición actual en el campo de la seguridad de la información de la empresa Edificadora BETA, mediante la aplicación de metodologías y buenas prácticas relacionadas con la gobernanza de TI y la gestión de los riesgos de la seguridad de la información. Es fundamental que las empresas cuya información está en su mayoría digitalizada puedan mantener en custodia mucha información (que pudiera ser confidencial o no) de forma segura. Para esto se requiere tanto de una cultura organizacional robusta que contemple y refuerce el buen manejo de dicha información, un plan de gestión de riesgos para garantizar la protección de la información, así como la continuidad del negocio en un entorno tan tierno (en lo que respecta a seguridad de la información) como el que se tiene en Costa Rica.

Debido a esto, se vio la necesidad analizar las políticas de la empresa para averiguar si cubren o no un buen manejo de la información, así como, preparar un análisis de riesgos tecnológicos para la empresa Edificadora BETA, tomando como base las buenas prácticas de la industria para el manejo de la información.

Con la información recopilada, fue posible crear una serie de recomendaciones y controles para mejorar el manejo de la información, así como implementar una serie de controles para disminuir los puntos de dolor de la empresa a algo más aceptable. El cómo se llegó a dichos controles se describe a lo largo del desarrollo de este documento.

1.1 Confidencialidad con respecto al uso de la información divulgada en este proyecto

La información confidencial y todos los derechos a la misma que han sido o serán divulgados al receptor de los datos, en este caso el autor de este proyecto de investigación, permanecerán como propiedad del divulgador cuya identidad es la Edificadora Beta. El receptor no obtendrá derecho alguno, de ningún tipo, sobre la información, ni tampoco ningún derecho de utilizarla, excepto para el objeto del presente acuerdo, que es la defensa del proyecto ante un jurado académico.

La información confidencial no podrá ser reproducida por ningún medio ni en ningún formato por el Receptor sin expresa autorización previa (por escrito) del divulgador, excepto por aquellas copias que el receptor pueda necesitar para hacer operativo este acuerdo.

Para finalizar, la información contenida en este escrito permanecerá confidencial por un periodo de 2 años, para dar al divulgador el tiempo suficiente para trabajar en las falencias de seguridad detectadas durante la evaluación.

Para efectos de protección a la empresa, la parte de la información mostrada sobre la infraestructura como nombre de los equipos, archivos específicos de configuración, así como rangos de IP han sido cambiados o no se muestran, con el fin de no revelar información sensitiva que podría ser utilizada por un atacante para infiltrarse en la red de la edificadora.

1.2 Antecedentes del problema a resolver – Seguridad de la información

Una realidad para cualquier empresa u organización moderna radica en que, los sistemas de información son necesarios tanto para producir valor agregado, así como para poder dar soporte al proceso de toma de decisiones por parte de la gerencia. Por tanto,

desde ese punto de vista es claro que toda organización requiere dichos sistemas de una u otra forma (se quiera o no) y requiere de dichos sistemas durante todo su ciclo de vida. Con el paso del tiempo, lo único que va a cambiar es la forma en que se implementarán estos sistemas.

El problema con dichos sistemas radica en que las empresas no ven aún la seguridad de la información como una necesidad en las organizaciones, sino más bien como un gasto al cual no se le presta una atención adecuada. Existen también casos, como el de la Edificadora Beta, en que la gerencia es consciente de que existen amenazas, pero no saben cómo identificarlas o tratarlas.

A nivel internacional, se pueden dar ejemplos de cómo empresas han sido altamente impactadas o incluso han desaparecido después de ser víctimas de brechas de seguridad de la información. Existen casos ampliamente conocidos de eventos tales como los que se citan a continuación para contextualizar el problema que se trata de resolver en este proyecto.

1.2.1 El sonado caso del "Ashley Madison"

El caso de Ashley Madison, es una de las brechas de seguridad de datos más resonantes de los últimos tiempos y una de las de mayor alcance, "cuyas implicaciones todavía se desconocen y es considerado uno de los casos más sonados del 2015". (Thomas, 2015, s. p.)

Ashley Madison, es básicamente una web para infieles, aunque la propia compañía asegura que no anima a nadie a ser infiel. De hecho, si tienes dificultades en tu relación de pareja, deberías buscar consejos y terapia, apunta Ashley Madison. Pero, como explica en

su página, si buscas a otra persona para satisfacer las necesidades que no cubre tu pareja, "estamos convencidos que nuestro sitio es el mejor lugar para empezar" (Rodríguez, 2015, s. p.)

Lo que sucedió con esta empresa de citas, es que fueron víctimas de un robo de datos de los clientes por parte de un grupo de *hackers*, que dejaron a los más de 30 millones de usuarios del sitio web impactados, debido a que su información personal, de contacto y tarjetas de crédito fue publicada sin ningún escrúpulo. Días después, el mismo grupo de *hackers* publicó un segundo bloque de información con documentos filtrados "que se centran en información corporativa sensible de Life Media, empresa matriz de Ashlie Madison" (Rodríguez, 2015, s. p.).

De acuerdo al diario español La Vanguardia, en su artículo del 15 de diciembre del 2015, la investigación reveló prácticas flojas de la compañía en materia de seguridad de datos, como el no mantener sus políticas de seguridad de la información o no usar la llamada autenticación multifactorial para garantizar el acceso remoto. Por tanto, se pudo determinar que hubo negligencia por parte de la empresa a la hora de proteger la información de sus clientes.

La brecha de seguridad que sufrió esta empresa tuvo repercusiones enormes, tanto económicas como de credibilidad y daño al nombre. Al final, la empresa aceptó pagar una multa 1.65 millones de dólares, una multa con un gran descuento (debido a la imposibilidad de pagar la multa original), para "poner fin a investigaciones estatales y federales" (La Vanguardia, 2016, s. p.).

1.2.2 Sony PlayStation Network (PSN), pérdida económica y repercusiones legales

Otro ejemplo de cómo las empresas se ven impactadas por brechas de seguridad, es el caso de la red de PlayStation de Sony. La revista Forbes, en su versión mexicana, publicó en agosto 25 del 2014 un artículo que describían en detalle los eventos acontecidos en el ataque contra la red PSN de la empresa japonesa Sony.

De acuerdo a Forbes, Sony anunció en su blog de PlayStation que su servicio PSN había "sido afectado por un ataque del tipo en que se niega el servicio a los usuarios, que saturó al sistema con tráfico, pero que no entró a la red ni accedió a la información de sus 53 millones de clientes." (Reuters, 2014, s. p.)

Se podría pensar que este tipo de ataques informáticos solamente se dan contra empresas con grandes ganancias, ubicadas en países de primer mundo. Sin embargo, en Costa Rica también se han dado casos como el que se detalla a continuación.

1.2.3 Caso en Costa Rica. Hackeo a la Caja Costarricense del Seguro Social (C.C.S.S)

Las brechas de seguridad no solo se dan fuera de Costa Rica, hoy en día, cualquier entidad que se encuentre conectada es vulnerable a un ciber ataque, ya sea por atacantes extranjeros o nacionales. El caso más sonado en Costa Rica en los últimos años corresponde al robo de más de 500 mil registros a la CCSS.

El diario costarricense La Nación, detalló en su versión digital del actualizado el 31 de agosto de 2015 la metodología empleada para obtener los datos, ya que según

escribieron “Para hacer el hackeo se utilizó un robot *software* para violentar las barreras de seguridad con las que cuenta la CCSS para proteger la información de sus usuarios en el Sicere.” (Avedaño, 2015, s. p.).

Según el diario, los sistemas de monitoreo y alarma de la CCSS detectaron la presunta acción delictiva a tiempo lo que permitió tomar las acciones legales a tiempo para dar con los responsables.

Semanas después, se dio con los presuntos responsables del robo que, de acuerdo al diario costarricense El Financiero en versión digital del 20 de septiembre del mismo año, fueron empleados del BAC San José. En el diario se detalló como: “la intromisión se dio por parte de funcionarios del Banco BAC San José, cuando enviaron solicitudes masivas de información y con *software* tipo robot lograron acceder a los datos de más de 522.000 afiliados” (Chacón, 2015, s. p.).

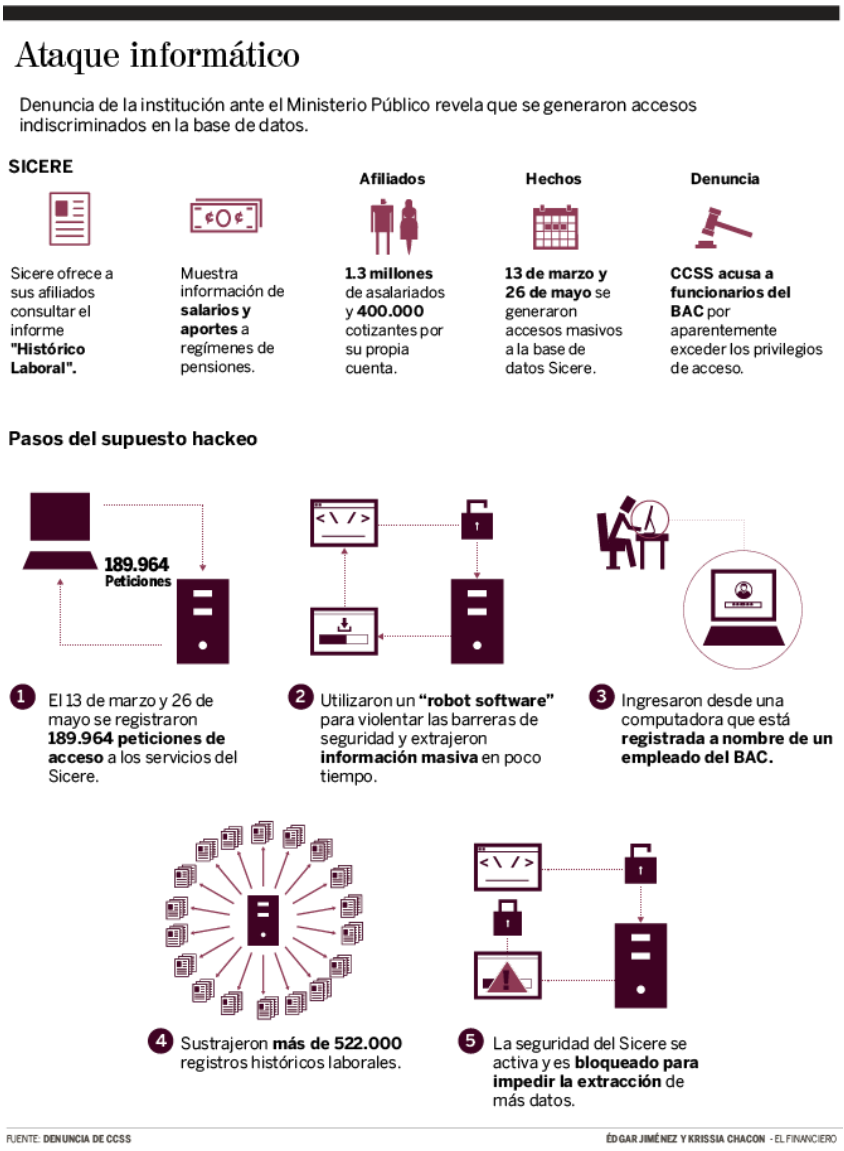


Figura 1 Cronología del robo de datos a la CCSS. Fuente: Denuncia de CCSS/El financiero.

A pesar de que se dio una detección del robo de los datos, nótese que fue detectada mucho tiempo después del hecho, por tanto nada se pudo hacer para impedirlo con los controles que tenía implementada la Caja. Con esto queda al descubierto que no solo a las

empresas fuera de Costa Rica son víctimas de Costa Rica y como el país tiene que tomar el tema de la seguridad de la información con seriedad.

1.3 Definición y descripción la situación de la Edificadora en cuanto la protección de sus datos.

Luego de citar ejemplos conocidos, en donde existió un impacto enorme tanto para la empresa como a los usuarios impactados, se puede hablar un poco sobre la realidad de la Edificadora, en donde la gerencia es consciente de que existen falencias en cómo se maneja la información e incluso han intentado asesorarse para estar menos expuestos, pero no han implementado una solución que les satisfaga.

La edificadora BETA se dedica a brindar servicios de ingeniería, gestión, construcción y desarrollo de obras civiles y de proyectos energéticos de alta calidad. Dicha empresa se encuentra ubicada en Avenida 1, Calle Los Rojas, Provincia de Alajuela, Ciudad Quesada.

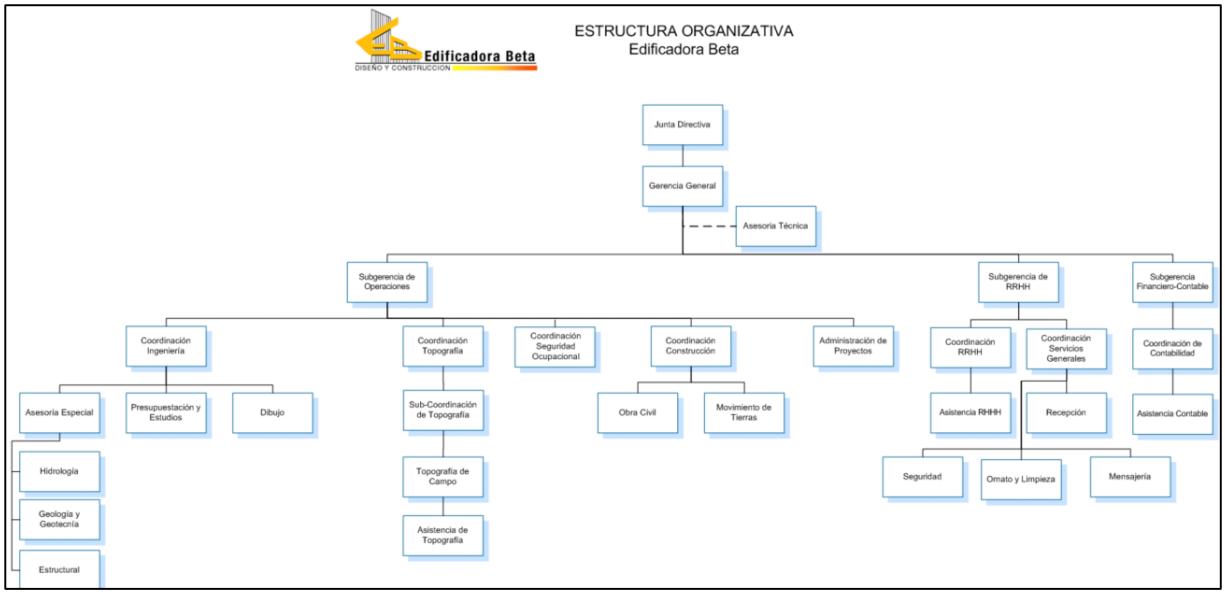


Figura 2 Organigrama de la empresa. Fuente Edificadora Beta.

Para efectos de la elaboración de este proyecto, la gerencia de la edificadora brindó como colaborador el Sr. Eduardo Mora Castro, encargado de TI de la empresa (emora@beta.cr).

1.3.1 Sobre la seguridad física de la edificadora

La Edificadora Beta está ubicada en una casa de dos casas de habitación acondicionadas y comunicadas internamente para la facilidad de las operaciones. Las instalaciones se encuentran cerradas por una cerca metálica, se tienen 2 puntos de entrada que permanecen cerrados hasta que se solicita la entrada a través de un timbre. Es ahí cuando la recepcionista verifica la identidad de la persona que desea ingresar mediante un intercomunicador y una cámara de vigilancia, una vez verificada la identidad de la persona, se le abre la puerta para que pueda llegar a la recepción.

El edificio cuenta con dos salidas, una de emergencia que se encuentra rotulada y cerrada todo el tiempo y solo se puede abrir desde adentro y la entrada principal en donde se encuentra la recepción.

Durante las visitas, se determinó la presencia de una alarma, la cual tiene conectados sensores de movimiento, así como sensores de humo en cada una de las áreas del edificio, adicionalmente se localizaron dos extintores clase B (derivados del petróleo, gasolina, *thinner*, aguarrás, líquidos combustibles) y C (equipo eléctrico energizado, corto circuito y cables) con instrucciones para su adecuado uso.

Para acceder a la documentación física de la empresa (planos, contratos, facturas, etc.) se debe de solicitar la llave de la biblioteca, como ellos lo llaman, que es un cuarto cerrado que cuenta con llave. Para obtener la llave se debe solicitar personalmente a la encargada de recursos humanos, que es quién guarda las llaves a los cuartos restringidos.

Con respecto a la seguridad física de los equipos, existe un cuarto de en donde estos se alojan de unos dos metros por dos metros. Dicho cuarto cuenta con aire acondicionado para mantener la temperatura de los equipos a raya, dicho cuarto está reforzado en concreto y se encuentra protegido por una puerta de hierro con llave, de la cual solo la persona encargada de las llaves y el encargado de TI tienen acceso. Los equipos que provee el Instituto Costarricense de Electricidad para el acceso al internet se encuentran ubicados en el casillero principal junto a los servidores.

Por la noche, el edificio queda cerrado y con las alarmas activadas, dichos dispositivos cuentan fuente de energía alternativa que les permite operar por cerca de 48 horas sin alimentación eléctrica, adicionalmente se cuenta con un guarda de seguridad que vigila el perímetro externo del edificio, dicha vigilancia transcurre durante toda la noche. Con respecto a la iluminación del perímetro externo de la empresa es adecuada, no se encontraron bloqueos de visión que permitan que un intruso se esconda fácilmente de los mecanismos de vigilancia.

1.3.2 Sobre la seguridad administrativa de la edificadora Beta

Con respecto a cómo se manejan los eventos administrativos se hicieron una serie de hallazgos que más adelante en el documento se detallaron y clasificaron para tomarlos en cuenta durante el análisis de riesgo y la elaboración de los controles.

La empresa cuenta con sus políticas administrativas algo generales, pero efectivas, sin embargo, no se cuenta con un programa de culturización constante en donde se refresque dichas políticas a los colaboradores de la empresa.

Con respecto al manejo de las contrataciones y los despidos, se denotó la ausencia de un procedimiento de "primer día en la oficina", en donde se les brinde una introducción a los estatutos de la empresa, así como las buenas prácticas de lo que se debe y no se debe hacer en la empresa a los nuevos colaboradores. Asimismo, tampoco se cuenta con un procedimiento formal de último día en la oficina, en el que se señalen la lista de actividades que se deben de hacer cuando se termina una relación laboral entre un colaborador y la empresa.

En la actualidad, la empresa no cuenta con la cultura de seguridad adecuada como para resguardar la información generada, así como las claves de acceso a los sistemas (principio de escritorio limpio).

La información de la empresa no se encuentra almacenada de una manera consistente, lo que tiene como consecuencia la creación de trabajo duplicado, copias de información vieja que no se necesita, pero es respaldada, así como sobre escritura de información lo que causa inconsistencias en las diferentes versiones.

El acceso a la información en el servidor de archivos está basado usuarios particulares y no en roles, complicando la administración de los permisos a los documentos.

1.3.3 Sobre la seguridad en materia tecnológica de la Edificadora Beta

La empresa cuenta con equipos portátiles para trabajar fuera de las instalaciones, dichos equipos cuentan accesos a la red de la empresa, correo electrónico configurado, así como documentos, planos y cotizaciones de gran importancia para la operación. Se observó que no todos los sistemas cuentan con cifrado de disco, por lo que la información queda desprotegida en caso de un robo del equipo.

También se descubrió que los usuarios de los equipos de la empresa, guardan todos sus documentos en sus discos duros locales y en algunas ocasiones, no realizan un respaldo de seguridad en el servidor de archivos, lo que expone dichos datos debido al robo o pérdida de una portátil o por el daño de un disco duro. Esto se debe a malas prácticas de los usuarios y no a que no cuenten con un medio en donde respaldar la información.

Uno de los gerentes ha manifestado su preocupación con respecto al acceso de los datos, ya que algunos de los colaboradores configuran el correo de la empresa (Edificadora Beta utiliza su correo electrónico montado en la plataforma de Google) en su dispositivo personal. Dichos dispositivos no cuentan con ningún tipo de cifrado, por tanto, en caso de robo o pérdida, podría comprometerse dicha información.

A la hora de identificar los dispositivos activos en la red, se verificó que no existe un inventario de dichos equipos para determinar si existe algún sistema no autorizado accediendo a los recursos de la red.

La conexión a internet de la empresa la reciben mediante dos enlaces de internet, un enlace de 25Mbs de bajada por 7Mbs de subida destinado a la operación del área de oficinas para actividades como envío de información a través de correo electrónico,

mientras que el otro enlace de 2Mbps de bajada por 1Mbps de subida, se utiliza para las conexiones externas de usuarios a través de un VPN montado en un servidor Windows 2008, el cual tiene la dirección IP pública configurada en su tarjeta de red principal. Se planea para el próximo año el ampliar el servicio de internet por uno simétrico, el obstáculo a la fecha ha sido la no disponibilidad de dicho servicio en San Carlos.

En lo que se refiere a la gestión de parches, el proceso es de tipo manual para servidores y a través de gestión automática para las estaciones de trabajo que corren Windows. La solución antivirus de la empresa corresponde a un *software* corporativo comercializado por la empresa Symantec (Symantec Endpoint Protection Small Business Edition v12.1), de forma que la administración de los paquetes de seguridad de la empresa se gestiona de manera centralizada mediante la consola de control instalada en el servidor de aplicación destinado a este fin.

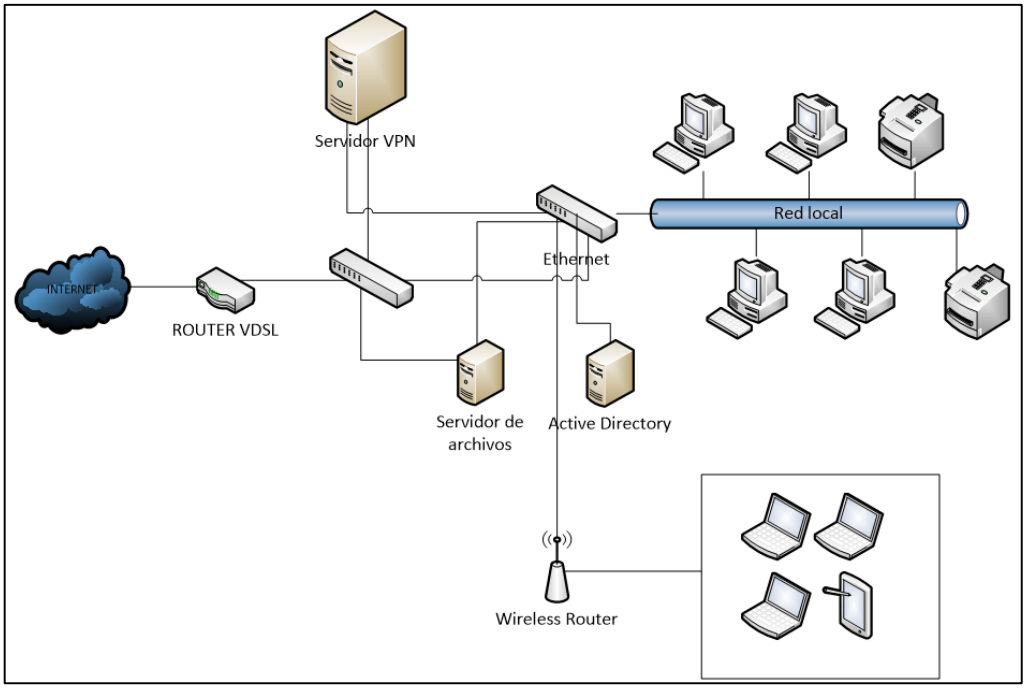


Figura 3 Diagrama lógico de la Infraestructura de red de la edificadora.

Fuente: Elaboración propia.

1.4 Justificación

Al día de hoy, a edificadora Beta, tiene una infraestructura tecnológica en constante cambio para poder cumplir con sus objetivos de negocio, de la cual dependen muchos de los procesos, dependencias y el funcionamiento tanto administrativo como técnico.

Gran parte de la información operativa de la empresa, se encuentra en los equipos del personal administrativo e ingenieros, otra parte en los buzones de correo, también existe información en formato físico y por último la que se encuentra almacenada en sistemas de información, pero se evidencia que no hay políticas de control que puedan proveer un

tratamiento adecuado de este valioso activo como es la información sensible de la Edificadora, que constituye su principal activo.

En la actualidad, las empresas deben considerar dentro de sus planes de gobierno interno la protección de la información mediante la creación de políticas y controles. La Edificadora debe de alinear sus objetivos operativos a asegurar el flujo de información, optimizar recursos y garantizar la confidencialidad, disponibilidad e integridad de la misma.

Se debe de realizar un análisis de riesgos para la Edificadora con el fin de garantizar mayor efectividad y eficiencia dentro de cada uno de los procesos y tener en cuenta que al conocer las fortalezas y debilidades se mejora el control y administración de recursos tecnológicos acorde a las buenas prácticas de la industria y que de esta forma se logren los objetivos institucionales.

1.5 Viabilidad

La viabilidad del proyecto está dada basada en las necesidades actuales de la empresa en estudio. Dicha empresa ya cuenta con equipo de red suficiente para el montaje y configuración de las soluciones de código abierto. Dichas soluciones se encuentran disponibles en líneas sin ningún cargo por su descarga o su utilización dentro de la empresa, siendo el mayor reto la implementación de las soluciones y el entrenamiento en su uso para los encargados de TI de la empresa, así como su aceptación como parte de la cultura organizacional.

1.5.1 Viabilidad técnica

Muchas de las mejoras que solventarían los problemas de seguridad de Beta, están basadas en cambios administrativos y en la implementación de tecnologías de código abierto, por tanto el proyecto es técnicamente viable.

1.5.2 Beneficiarios del proyecto

El principal beneficiario del proyecto es la Edificadora Beta, que con la puesta en marcha de los controles sugeridos mejorará enormemente la seguridad sobre su activo principal, que es su información.

1.5.3 Tecnología del proyecto

Las tecnologías que se utilizarán para el desarrollo de este proyecto son metodologías de uso gratuito, así como herramientas de código libre como por ejemplo la distribución de Linux Kali, que se utilizará para localizar los activos conectados a la red y sus vulnerabilidades a ataques informáticos.

1.5.4 Evaluación económica

Como se mencionó en el punto anterior, como las tecnologías que se implementarán en la empresa son de código de libre distribución, los costos son bastante bajos y lo que se requiere es mucho tiempo y evaluación por parte del autor de este proyecto, por tanto el proyecto es económicamente viable para la Edificadora Beta.

1.5.5 Retorno de la inversión

El retorno de la inversión en las soluciones de seguridad se da cuando NO se materializa la explotación de una vulnerabilidad por parte de una amenaza, por tanto, el

retorno de la inversión consiste en que la empresa no sea víctima de una brecha de seguridad que comprometa su información o su reputación.

1.6 Objetivos

1.6.1 Objetivo general

Confeccionar una propuesta para mejorar la protección de la información de la Edificadora Beta, así como la implementación parcial de los controles y procedimientos sugeridos en dicho análisis.

1.6.2 Objetivos específicos

a) Analizar marcos metodológicos de gobierno corporativo y de gestión de riesgos para ser aplicados a una empresa costarricense. En este caso, la empresa elegida es la Edificadora Beta.

b) Estudiar las políticas y procedimientos actuales de la Edificadora, para la identificación de las fortalezas y posibles deficiencias en el modelo actual y para la propuesta de las mejoras correspondientes basadas en las buenas prácticas de la industria.

c) Identificar las áreas de preocupación de la gerencia con respecto al manejo actual de sus datos, para la confección de un plan de acción que permita solucionarlas.

d) Clasificar los principales activos que forman parte del modelo de negocio del centro de tecnología de la constructora, como equipos utilizados, lugar de trabajo y *software* disponible con el fin de darles valor a estos para que la

elección de los recursos requeridos sea la adecuada para proteger dichos activos.

e) Identificar las principales amenazas que afectan a los activos citados anteriormente, que pudieran afectar la confiabilidad, integridad y la disponibilidad de la información contenida.

f) Proponer controles que minimicen los riesgos encontrados, recomendar el ciclo de vida y mantenimiento de los controles, así como el entrenamiento requerido para el buen uso de los mismos.

1.7 Alcances y limitaciones

1.7.1 Alcances

Este trabajo tiene como alcance la elaboración de la propuesta a la Edificadora Beta de cómo proteger su información, así como la primera fase de implementación, en donde las recomendaciones más críticas serán tratadas si se cuenta en el momento con los recursos disponibles y para las menos críticas, quedará en manos del departamento de TI de la edificadora un documento con el plan de acción a seguir para remediarlas.

Mediante el desarrollo de este escrito, se pretende generar consciencia sobre la necesidad en las organizaciones de contar con gobierno corporativo, que a la vez contemple una estrategia de gestión de riesgos con enfoque estructurado para manejar la incertidumbre dada por las diferentes amenazas que se encuentran en el día a día de las organizaciones y más en concreto, en la Edificadora Beta. Se toma en consideración que para cualquier propuesta e implementación exitosa se requiere del apoyo de la gerencia para llevar a

término la solución y que llegue a adaptarse a la cultura de la empresa. En este caso, la gerencia de la edificadora ha estado de acuerdo en permitir la elaboración de esta propuesta y se ha comprometido a tomar seriamente las recomendaciones resultantes de este documento.

1.7.2 Limitaciones

1.7.2.1 Tiempo: la adopción de la seguridad de la información en las empresas no es un proceso que se dé de la noche a la mañana y la edificadora no es la excepción.

1.7.2.2 Falta de entrenamiento del personal. Como ya es ampliamente conocido la gestión de seguridad de la información, el usuario final representa el eslabón más débil en la cadena y capacitación de los usuarios es un factor determinante para el éxito de la propuesta, dicha capacitación es un proceso constante que debe de adoptarse de manera gradual dentro de la organización.

1.7.2.3 Recurso económico: Si bien es cierto, mediante el uso de tecnologías de código abierto permitirá bajar el costo de implementación algunos de los controles, estos no costos no llegarán a cero e incluso para implementarlos, podrían requerir la compra de equipo adicional para poder hacerlos efectivos.

1.8 Marco de referencia organizacional

La información que se describe a continuación tiene como fuente la documentación proporcionada por la gerencia de Beta para el desarrollo de este proyecto.

1.8.1 Historia

Edificadora Beta es una empresa costarricense fundada el 28 de enero de 1987, cuenta con un sólido y experimentado equipo de profesionales y técnicos de planta, así como consultores externos que le permiten a la empresa brindar servicios de ingeniería con gran eficiencia y calidad.

1.8.2 Tipo de negocio y mercado meta

La edificadora se dedica a brindar servicios de asesoría, diseño, administración y construcción de obras civiles en general, aunque desde 1991, Edificadora Beta se ha concentrado en la búsqueda, diseño, gestión y construcción de proyectos energéticos. El mercado meta es toda empresa que requiera servicios de ingeniería para la construcción de sus obras.

1.8.3 Misión, visión y valores

1.8.3.1 Misión

Desarrollar proyectos de infraestructura buscando satisfacer las necesidades de nuestros clientes desde antes hasta luego de terminado el proyecto, ofertando diseños a la vanguardia cumpliendo con los estándares de calidad, así como innovar con las últimas tendencias encontradas en el sector de la construcción, buscando mejorar los procesos para hacer más eficiente el producto final.

1.8.3.2 Visión

Ser una empresa líder en el sector de servicios de asesoría, diseño, administración y construcción de obras civiles, con un equipo comprometido, evolucionando constantemente nuestros servicios para ofrecer productos innovadores que satisfagan las necesidades de los

clientes, con altos estándares de calidad, cumplimiento, diseño y conciencia de servicio al cliente que garanticen solidez de la empresa.

1.8.3.3 Valores

a) Enfoque en el desarrollo del negocio a largo plazo sin perder de vista la necesidad de obtener continuamente resultados sólidos para nuestros clientes.

b) Buscamos la satisfacción de nuestros clientes sirviéndolos no solo antes y durante el proceso de cada proyecto sino luego de la entrega de los mismos, retándonos continuamente para alcanzar los máximos niveles de calidad en nuestros proyectos.

c) Mejora continua hacia la excelencia como forma de trabajar, buscando innovación.

d) Compromiso con una ética laboral sólida, integridad y honestidad, así como con el cumplimiento de las normas de control de calidad y diseño existentes.

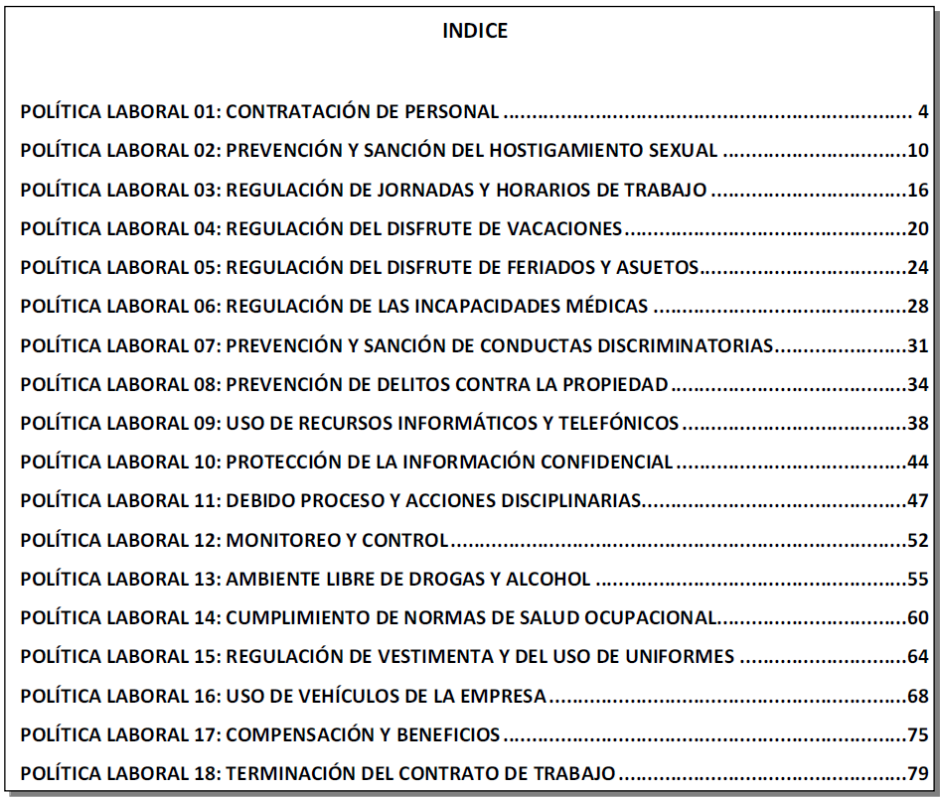
e) Velamos por el bienestar y desarrollo de los trabajadores considerando sus opiniones y respetándolos como personas.

f) Perseguimos permanentemente la incorporación de nuevas modalidades de trabajo, la utilización de nuevos materiales y la incorporación de tecnología en todas las áreas de nuestra empresa, ya que es condición indispensable para alcanzar el liderazgo.

g) Puntualidad con el cumplimiento de las entregas de los proyectos.

1.8.3.4 Políticas institucionales

Con respecto a las políticas institucionales, la empresa cuenta con un manual de políticas firmado por el gerente general de la empresa que consta de 82 páginas en donde se describen de manera general las expectativas y compromisos que la gerencia tiene hacia sus colaboradores.



INDICE

Figura 4 Índice parcial del manual de políticas de Edificadora Beta.

Fuente: Edificadora Beta

Para efectos de este proyecto, las políticas que se analizarán para comprobar que se protege la información de la empresa son las siguientes:

Política Laboral 8 - Prevención de delitos contra la propiedad: esta política habla en concreto de la protección a los activos físicos de la empresa, tales como herramientas, equipo, vehículos, de cuáles son las obligaciones de los colaboradores y las posibles sanciones por incumplimiento de estas.

Política Laboral 9 - Uso de recursos informáticos y telefónicos: aquí se denomina como recursos informáticos al internet, contraseñas a los sistemas de información de la empresa y de cómo los colaboradores deben comportarse cuando utilicen dichos recursos, así como de la prohibición del uso de estos para actividades no propias del día a día de los colaboradores, tales como el uso de redes sociales, participación en foros, realizar copias del *software* perteneciente a la empresa, uso adecuado del correo electrónico de la empresa (por ejemplo el no envío de correo no solicitado [*spam*] o cadenas de correos a particulares). En lo que respecta al uso del teléfono, se establecen los lineamientos para el uso aceptable de este recurso para llamadas de carácter laboral únicamente. De nuevo, al final de la política se hace mención de las medidas disciplinarias en caso de incumplimiento. En esta política tampoco se menciona la información como un recurso, por tanto, no la cubre.

Política Laboral 10 Protección de la información confidencial: en términos generales, la política de protección de datos de la empresa habla sobre el profesionalismo que deben tener los colaboradores en lo que respecta al manejo de datos de la información de la empresa y que mantener protegida dicha información es obligatorio, así como de las sanciones correspondientes a los incumplimientos. Sin embargo, cuando se le consultó al gerente si existía algún grado de clasificación de la información, la respuesta fue negativa, por tanto, la política general existe, pero no es posible aplicarla consistentemente.

Política Laboral 12 Monitoreo y control: esta política de acatamiento obligatorio se refiere a la vigilancia que puede ejercer la empresa sobre sus colaboradores, está enfocada en los activos físicos, los colaboradores pueden ser revisados para entrar o salir de las instalaciones, así como las medidas disciplinarias por incumplimiento. Sin embargo, en ningún momento se contempló el monitoreo y control de los activos digitales de la empresa.

1.9 Estado de la cuestión - Estado de la Ciber Seguridad en Costa Rica

El autor de este documento decidió realizar una investigación sobre la situación actual de seguridad de la información en Costa Rica de las empresas PYME locales, la madurez de estas, si existe en el país una consciencia sobre este tema y una debida gestión de riesgos con sus respectivos controles.

Inicialmente, para realizar el sondeo se utilizó Google Académico (scholar.google.com) en donde se aplicaron los siguientes criterios de búsqueda.

Inicialmente se utilizaron los criterios:

+ciberseguridad +"costa rica" +herramientas

Lo cual regresó un total de 133 resultados.

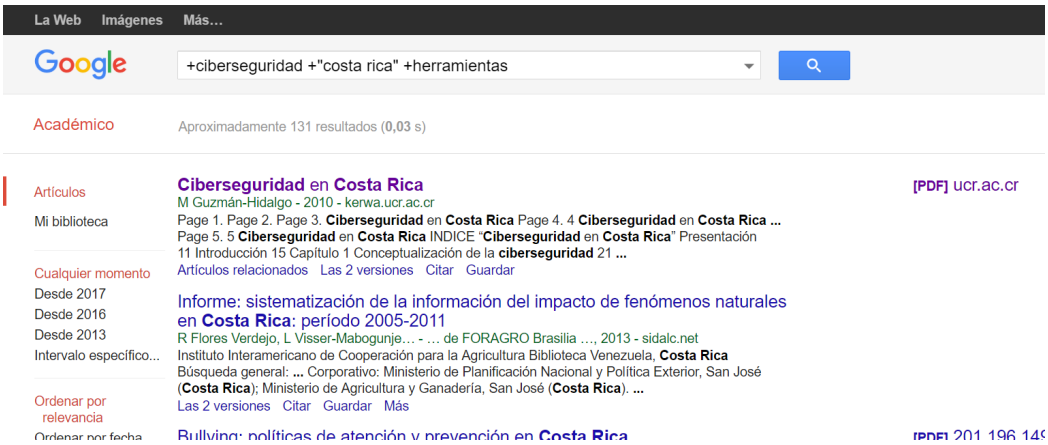


Figura 5 Resultados del Scholar de Google

Se agregó más parámetros a la búsqueda "site:cr" para delimitar a dominios en Costa Rica y se obtuvieron 11 resultados.

Figura 6 Resultados del Scholar de Google con filtros extra

Un documento de valor recuperado para ver y analizar los estudios que se han hecho en Costa Rica en lo que respecta a la seguridad de la información, corresponde al libro de libre distribución Ciberseguridad en Costa Rica, de la editorial de la Universidad de Costa Rica. Dicho libro cuenta con múltiples autores que describen una serie de situaciones que involucran las consecuencias de la pérdida de datos y de cómo los costarricenses en general no tienen la cultura suficiente para hacer frente a estas amenazas. Adicionalmente se menciona el hecho de que en Costa Rica se cuenta con la infraestructura adecuada para el manejo a nivel nacional de la firma digital para documentos, sin embargo es poca la gente que tiene conocimiento de esto y los medios para solicitarla y utilizarla. Un dato importante es que de acuerdo al MICITT y a Marcelo Jenkins, Ministro de Ciencia, Tecnología y Telecomunicaciones quién detalló que a la fecha:

> Más de 123 mil costarricenses cuentan con su certificado de firma digital, lo que constituye un gran avance en materia de digitalización de procesos en el país. Gracias a su Firma Digital, esta población puede realizar más de 250 trámites distintos en más de 55 instituciones públicas, bancarias y comerciales que ya utilizan el sistema (MICITT, 2015).

Sin embargo, la firma lo que permite es validar que un documento no ha sido adulterado, pero, ¿qué pasa con la protección de los datos? ¿cómo se protegen del robo de la información? No se puede negar que existe un esfuerzo importante por parte del MICITT para impulsar estas tecnologías. Sin embargo, la protección de la información digital en el país no se encuentra en su mejor momento debido a la falta de conocimiento en el campo.

Luego se realizaron nuevas búsquedas relacionadas con el manejo de gobierno dentro de las empresas, así como de la gestión de riesgos sobre la información orientada a Costa Rica. Los resultados se detallan a continuación.

Para esta nueva búsqueda, se utilizaron los criterios:

+"gobierno" +"costa rica" "seguridad de la información" +"gestión de riesgos" site:cr

Lo cual regresó un total de 27 resultados.

Esta búsqueda arrojó resultados interesantes como el Desarrollo de un compendio de los contenidos regulatorios en Costa Rica y de gobierno de la seguridad de la información, con el fin de establecer una guía de auditoría para evaluar las amenazas técnicas sobre los servicios de “Cloud Computing” direccionados al modelo de servicio IAAS, creado por Carolina Odio González, Master en Auditoría de Tecnologías de Información. En este se señalan una serie de buenas prácticas para la transición de datos a la nube de una manera segura, como se mencionó anteriormente dicho documento

constituye una guía valiosa en términos generales, sin embargo no incluye una implementación que permita mostrar los beneficios de estas recomendaciones.

Luego, mediante el agregado de algunos operadores para filtrar mejor los resultados se obtuvieron 5 resultados relevantes tales como:

+"implementación" +"gobierno corporativo" +"costa rica" "seguridad * información" +"gestión de riesgos" site:cr

En donde los documentos encontrados correspondieron a proyectos de graduación escritos por estudiantes aspirantes al grado de Maestría Profesional en Auditoría de Tecnologías de la Información. Luego de leer los resúmenes de dichos documentos, todos tuvieron como factor común el hecho que son propuestas de controles para mejorar la gobernanza dentro de las empresas en donde fueron realizadas, aplicando los marcos de

buenas prácticas respectivos de acuerdo al tipo de negocio, orientados al área de auditoría sin enfocarse en soluciones de índole técnico.

El presente proyecto pretende realizar el respectivo análisis de la situación actual de la empresa escogida, crear las recomendaciones a seguir para mejorar la seguridad de la información basado en las buenas prácticas, así como la implementación de controles de índole tecnológico, basándose principalmente en herramientas de código abierto para así, facilitar la implementación de estos.

Capítulo 2: Marco teórico

En la sección actual se definirán algunas de las definiciones de uso obligatorio con respecto al proyecto en desarrollo, con base en los documentos de buenas prácticas vigentes aceptadas internacionalmente para el control de la información en las TI y sus riesgos, como por ejemplo COBIT (Objetivos de Control para Información y Tecnologías Relacionadas), su adaptación al país, por parte de la Contraloría General de la República de Costa Rica (Normas técnicas para la gestión y el control de las Tecnologías de Información N-2-2007-CO-DFOE) así como la serie de normas ISO/IEC 27000, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, como lo es la edificadora Beta.

2.1 Normas internacionales para la gestión de la seguridad de la información

El portal especializado en las normativas ISO 27000, resume en uno de sus documentos publicados el origen de cada una de las normativas ISO (ISO27000.ES). En dicho documento, se describe el alcance de cada uno de las normativas y su evolución en el tiempo. Para efectos de este proyecto es importante que el lector conozca un poco sobre estas normativas, ya que facilitarán la comprensión de las recomendaciones basadas en buenas prácticas sugeridas a la edificadora.

2.1.1 Norma BS 7799 de BSI

El portal especializado en las normativas ISO 27000, narra de manera cronológica el origen de la norma BS 7799 (ISO27000.ES), el cual se describe a continuación.

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de julio de 2007, manteniendo el contenido, así como el año de publicación formal de la revisión.

En marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

2.1.2 La serie 27000

Con respecto a la serie de normas 27000, el portal especializado en las normativas ISO 27000, prosigue con su narración cronología de la evolución de las normas 27000 (ISO27000.ES), el cual se describe a continuación.

ISO 27000: En fase de desarrollo; su fecha prevista de publicación es noviembre de 2008. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.

ISO 27001: Publicada el 15 de octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser

obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

ISO 27002: Desde el 1 de julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org.

ISO 27004: En fase de desarrollo; su fecha prevista de publicación es noviembre de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.

ISO 27005: Publicada el 4 de junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000. En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.

ISO 27006: Publicada el 13 de febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

Luego de un breve estudio de las normas ISO, queda claro de que muchas de las metodologías a seguir para una buena gestión de TI ya existen, por tanto no hay necesidad de reinventar buenas prácticas, sino que puede hacerse un reciclaje adecuado del conocimiento en este campo, lo que ahorrará tiempo y esfuerzo en su implementación, además facilitará una adopción global, ya que todas estas normas son estándares que los auditores y responsables de gestión de TI deberían conocer y entender, lo que facilita su gestión y mantenimiento.

2.1.3 COBIT 5

ISACA, una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información creadores y custodios del marco de trabajo de COBIT en su versión 5.0 definen este marco como “COBIT 5 es un marco exhaustivo de principios, prácticas, herramientas y modelos de análisis mundialmente aceptados, que pueden ayudar a cualquier empresa a abordar aspectos críticos relacionados con el gobierno y la gestión de la información y tecnología.” (ISACA, 2012)

El estudio del marco de COBIT facilita la mejor comprensión de las recomendaciones basadas en buenas prácticas brindadas por los profesionales en la seguridad de la información. Si una empresa desea certificarse en COBIT, deberá de comprar el libro de normas y contratar a un auditor que les ayude con la implementación y certificación. Para efectos de la Edificadora Beta, no existe la intención de certificarse, solamente la de mejorar sus prácticas en lo que respecta a la gestión de su información, por tanto, la compra de dicho documento no es requerida.

2.2 Metodologías de análisis de riesgos.

2.2.1 Octave

OCTAVE es una metodología de análisis de riesgos desarrollada por la Universidad Carnegie Mellon, específicamente por la división CERT en los años 1999-2000 y estudia los riesgos en base a tres principios Confidencialidad, Integridad y Disponibilidad. Esta metodología se emplea por distintas agencias gubernamentales tales como el Departamento de Defensa de los Estados Unidos y está pensada en grandes organizaciones con 300 empleados o más. Sobre esta metodología, se cita textualmente la descripción de los creadores:

> El método OCTAVE es un método utilizado para evaluar las necesidades de seguridad de la información de una organización. OCTAVE Allegro es el método más recientemente desarrollado y activamente apoyado. Este método se basa en dos versiones anteriores denominadas OCTAVE Original y OCTAVE-S.
>
> Los métodos OCTAVE son autodirigidos, flexibles y evolucionan. Utilizando OCTAVE, equipos pequeños a través de las unidades de negocio y las de TI trabajan juntos para satisfacer las necesidades de seguridad de la organización. El método se puede adaptar al entorno de riesgo único de la organización, a los objetivos de seguridad y resistencia y al nivel de habilidad. OCTAVE mueve a la organización hacia una visión de seguridad operativa basada en el riesgo y aborda la tecnología en un contexto empresarial. (CERT - Carnegie Mellon University)
>
> OCTAVE Allegro se centra en los activos de información. Los activos importantes de una organización son identificados y evaluados en base a los activos de información a los que están conectados. Este proceso elimina la confusión potencial sobre el alcance y reduce la posibilidad de que la recopilación y el análisis extensos de datos se realicen para los activos que están mal definidos, fuera del alcance de la evaluación o que necesitan una mayor descomposición.
>
> OCTAVE Allegro se puede llevar a cabo en un ambiente de colaboración y estilo de trabajo y es adecuado para aquellos que quieren realizar la evaluación de riesgos sin mucha participación de la organización. OCTAVE Allegro consta de ocho etapas organizadas en cuatro fases:
>
> 1. Desarrollar criterios de medición de riesgo consistentes con la misión de la organización, los objetivos y los factores críticos de éxito.

2. Crear un perfil de cada activo de información crítico que establezca límites claros para el activo, identificar sus requisitos de seguridad e identificar todos sus contenedores.
3. Identificar las amenazas a cada activo de información en el contexto de sus contenedores.
4. Identificar y analizar los riesgos de los activos de información y comenzar a desarrollar enfoques de mitigación (controles).

Luego de analizar esta metodología, cabe resaltar que coincide con otras en las que se resalta la necesidad de estudiar los activos a los cuales hay que proteger, categorizarlos, así como asignarles valor para poder decidir el tipo de controles que hay que aplicarles para protegerlos, así como en nivel de riesgo deseado al final del avalúo.

2.2.2 Metodología MAGERIT

Otra metodología para el análisis de los riegos en una organización corresponde a MAGERIT v.3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información versión 3), que según sus creadores del Consejo Superior de Administración Electrónica de España:

> Nace como respuesta a la percepción de que la Administración, y en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.” (Consejo Superior de Administración Electrónica de España, 2012)

La idea general de MAGERIT es que pueda ayudar a todos aquellos que trabajan con información digital y sistemas informáticos y puedan desarrollar medidas adecuadas para protegerla utilizando las buenas prácticas sugeridas por esta metodología.

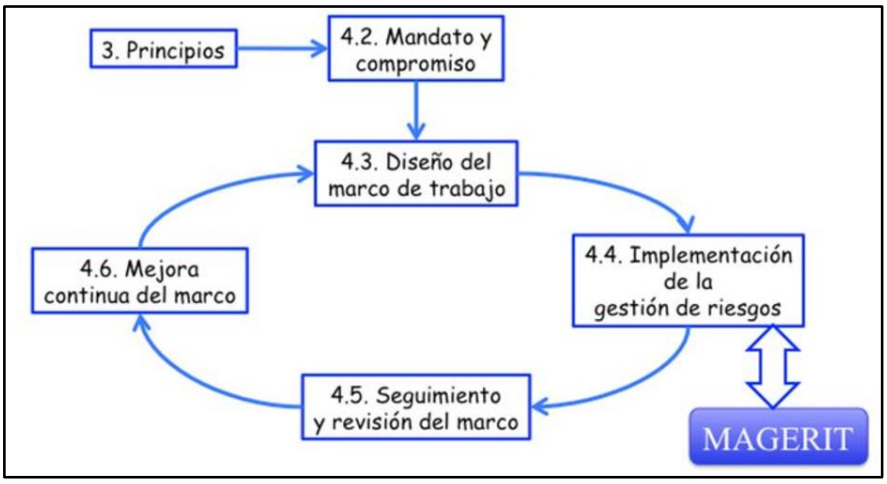


Figura 7 ISO 31000 - Marco de trabajo para la gestión de riesgos.

Fuente: administracionelectronica.gob.es

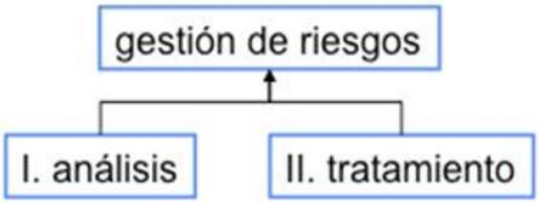


Figura 8 Gestión de riesgos MAGERIT:

Fuente: administracionelectronica.gob.es

El Consejo Superior de Administración Electrónica de España (Consejo Superior de Administración Electrónica de España, 2012), menciona los objetivos directos de esta metodología.

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.
4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Figura 9 Enfoque de Magerit para el manejo de los riesgos.

Fuente: Libro I de Magerit de la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica de España.

Dado a que MAGERIT es una metodología de carácter público, perteneciente al Ministerio de Hacienda y Administraciones Públicas; su utilización no requiere autorización previa del mismo, por tanto se puede utilizar para desarrollar el análisis de

riesgo de la edificadora para determinar en donde están las áreas de dolor de la compañía y diseñar los controles requeridos.

2.2.3 Herramientas de código abierto a utilizar en el proyecto

Una vez que se han enumerado herramientas metodológicas de buenas prácticas de la industria para gestionar tanto TI como la gestión de riesgos en las organizaciones, se procede a introducir las herramientas de *software* de código libre que ayudarán en el desarrollo de este proyecto.

El *software* de código abierto está desarrollado por y para la comunidad de usuarios. En la actualidad existen una gran variedad de aplicaciones de código abierto, desde aplicaciones de productividad hasta *software* de calendario o correo electrónico, así como herramientas que facilitan los procesos de protección de la información y que serán utilizadas durante el desarrollo de este proyecto.

Sobre las razones del porque se debería de utilizar aplicaciones de código abierto para el manejo de las soluciones de seguridad, aparte del factor económico, Bruce Schneier, criptográfico y experto en seguridad informática afirma con respecto a las herramientas de código abierto que:

> Nunca he entendido el alboroto actual sobre el movimiento del *software* de código abierto. En el mundo de la criptografía, consideramos que el código abierto es necesario para una buena seguridad; Que tenemos durante décadas. La seguridad pública es siempre más segura que la seguridad propietaria. Es cierto para algoritmos criptográficos, protocolos de seguridad y código fuente de seguridad. Para nosotros, el código abierto no es solo un modelo de negocio; es una práctica de ingeniería inteligente (Schneier, 1999, s. p.).

2.2.3.1 Kali Linux

Offensive Security, creadores de esta distribución de Linux describe a Kali Linux como:

> Una distribución Linux basada en Debian destinada a pruebas avanzadas de penetración y auditoría de seguridad. Kali contiene varios centenares de herramientas que están orientadas a diversas tareas de seguridad de la información, tales como pruebas de penetración, investigación de seguridad, computación forense e ingeniería inversa. Kali Linux es desarrollado, financiado y mantenido por Offensive Security, una compañía líder en capacitación en seguridad de la información (Offensive Security, s. f., s. p.).

Entre las herramientas incluidas en la distribución de Kali, se utilizarán las siguientes.

i. Nmap: herramienta de código abierto para exploración de red y auditoría de seguridad. (nmap.org, s.f.)

ii. Zenmap: interfaz gráfica oficial de Nmap, el conocido programa de código abierto para hacer escaneo de puertos a fondo de cualquier equipo conectado. (nmap.org, s.f.)

iii. aircrak-ng: es un conjunto completo de herramientas para evaluar la seguridad de la red WiFi. (ircrack-ng, s.f.)

iv. Wireshark: es una herramienta multiplataforma utilizada para realizar análisis sobre paquetes de red. La utilización de esta herramienta puede parecer de gran complejidad en un principio, pero es de gran utilidad una vez conocida su interfaz y su forma de operar. Existen diferentes usos para los cuales puede aplicarse Wireshark. Dentro del análisis dinámico de códigos maliciosos se la utiliza para detectar conexiones ocultas del propio malware con direcciones remotas para obtener otros archivos, para reportarse a un panel de control en caso de una botnet, entre otras variantes. (Catoira, 2013)

2.2.3.2 Keepass

Dominik Reichl, autor de la herramienta KeePass la describe como:

> Un gestor de contraseñas de código abierto gratuito, que ayuda a gestionar sus contraseñas de forma segura. Puede poner todas sus contraseñas en una base de datos, que está bloqueada con una clave maestra o un archivo de clave. Así que solo tienes que recordar una sola contraseña maestra o seleccionar el archivo clave para desbloquear toda la base de datos. Las bases de datos se cifran utilizando los

mejores y más seguros algoritmos de cifrado actualmente conocidos (AES y Twofish) (Reichl, s. f., s. p.)

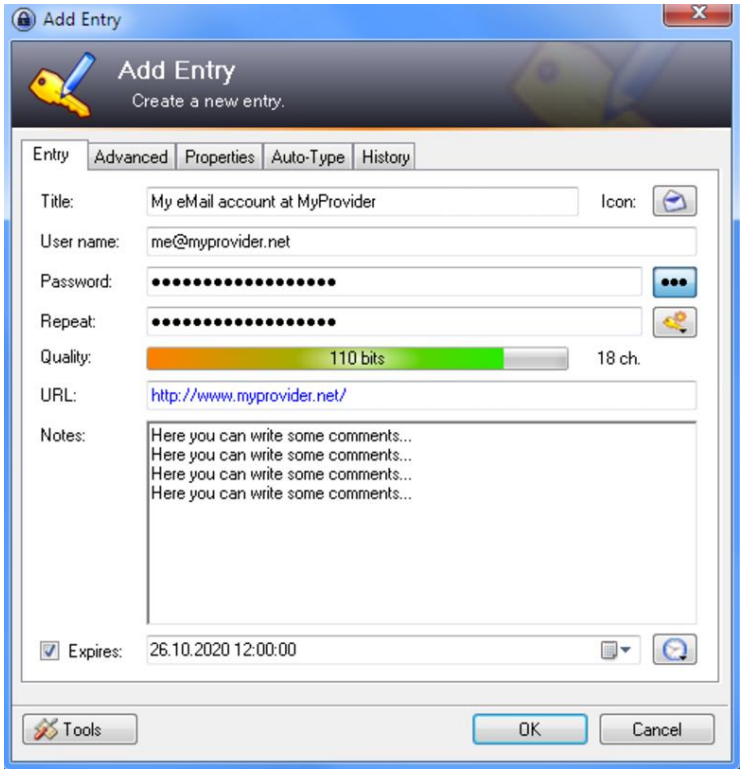


Figura 10 Ejemplo de gestión de claves en la herramienta de Keepass.

Fuente: Página del autor

2.2.3.3 FreeNAS

De acuerdo a los creadores de esta solución de almacenamiento la definen como:

> FreeNAS es un sistema operativo que se puede instalar en prácticamente cualquier plataforma de *hardware* para compartir datos a través de una red. FreeNAS es la forma más sencilla de crear un lugar centralizado y fácilmente accesible para sus datos. Utilice FreeNAS con ZFS para proteger, almacenar, copia de seguridad, todos sus datos. FreeNAS se utiliza en todas partes, para el hogar, la pequeña empresa y la empresa (FreeNAS, 2017).

Según su documentación interna, entre las ventajas que ofrece FreeNAS, como solución de gestión de archivos sobre otro tipo de sistemas de archivos, hay que destacar que:

- Brinda una interfaz relativamente sencilla de utilizar en un entorno web que permite administrar el sistema de almacenamiento en red.
- Los requisitos de *hardware* realmente son bajos, se puede instalar con 128 megas de RAM, aunque dependiendo de las funciones avanzadas que se utilicen, estas necesidades de memoria podrían aumentar hasta 8192 megas si se usa compresión de datos.
- Permite adoptar distintas configuraciones, ya sea en RAID[1] 0, 1 o 5 para dar más seguridad al almacenamiento de datos o si se prefiere aumentar la capacidad de almacenamiento.
- Permite cifrar el contenido de los discos duros, las comunicaciones para la transferencia de los archivos, así como crear usuarios y grupos con distintos privilegios para gestionar el NAS, ya sea como invitados o administradores manteniendo un sistema de permisos muy completo, mejorando así, la protección de la información.

Vale la pena aclarar algunos conceptos que son propios de la arquitectura de un NAS, como son:

ZFS: De acuerdo con Canonical, compañía detrás de la distribución de Linux Ubuntu, ZFS es:

[1] Redundant Array of Independent Disks, tecnología que permite tener redundancia de la información almacenada en los discos.

Un sistema de archivos combinado y un gestor de volumen lógico diseñado e implementado por un equipo de Sun Microsystems dirigido por Jeff Bonwick y Matthew Ahrens. Su desarrollo comenzó en 2001 y se anunció oficialmente en 2004. En 2005 se integró en el tronco principal de Solaris y se lanzó como parte de OpenSolaris. Actualmente, a partir de enero de 2015, es nativo de Solaris, OpenSolaris, OpenIndiana, Illumos, Joyent SmartOS, OmniOS, FreeBSD, sistemas Debian GNU / kFreeBSD, NetBSD, OSv y compatible con Mac OS con MacZFS. El nombre "ZFS" representaba originalmente "Zettabyte File System". Actualmente puede almacenar hasta 256 ZiB (zebibytes) (Canonical, 2017).

Adicionalmente se deben mencionar sus tres objetivos de diseño principales que de acuerdo a la documentación oficial de FreeBSD son:

Integridad de datos: Todos los datos incluyen una suma de comprobación de los datos. Cuando se escriben datos, la suma de comprobación se calcula y se escribe junto con ella. Cuando los datos se vuelven a leer, la suma de comprobación se calcula de nuevo. Si las sumas de comprobación no coinciden, se ha detectado un error de datos. ZFS intentará corregir automáticamente los errores cuando la redundancia de datos esté disponible.

Almacenamiento agrupado: los dispositivos de almacenamiento físico se agregan a un grupo y el espacio de almacenamiento se asigna desde dicho grupo compartido. El espacio está disponible para todos los sistemas de archivos y se puede aumentar añadiendo nuevos dispositivos de almacenamiento a la agrupación.

Rendimiento: múltiples mecanismos de almacenamiento en caché proporcionan un mayor rendimiento. ARC es una caché de lectura basada en memoria avanzada. Se puede agregar un segundo nivel de caché de lectura basado en disco con L2ARC y el caché de escritura síncrono basado en disco está disponible (Rhodes, Jude, Reuschling, & Block, 2017).

2.2.3.4 SQUID

SQUID es una herramienta de código abierto con muchísimos años en el mercado, de acuerdo a su página oficial, se puede extraer su definición y sus características que se citan a continuación.

SQUID es un proxy de almacenamiento en caché para la Web que admite HTTP, HTTPS, FTP y más. Reduce el ancho de banda y mejora los tiempos de respuesta mediante el almacenamiento en caché y la reutilización de las páginas web solicitadas con frecuencia. Squid tiene amplios controles de acceso y hace un gran acelerador de servidor. Se ejecuta en la mayoría de los sistemas operativos

> disponibles, incluyendo Windows y está bajo la licencia de GNU GPL (Comunidad SQUID, 2013).

SQUID, al ser un proyecto guiado por la comunidad y altamente activo, tiene la ventaja que recibe constantemente actualizaciones de seguridad que le permite ser una plataforma segura, esto se puede comprobar leyendo los CVE (Common Vulnerabilities and Exposures) publicados constantemente en su página web con su respectiva corrección.

2.2.3.5 IPCop

Como solución de cortafuegos para la edificadora, se puede utilizar IPCop, que de acuerdo a la página web de sus creadores se define como:

> IPCop es una Distribución Linux especializada; completa, configurada y lista para proteger su red. Además, está distribuida bajo licencia GNU General Public License, con todo el código fuente disponible para descargarlo, revisarlo o incluso ser modificado y/o recompilado por usted mismo para sus necesidades personales o por razones de seguridad (Ezquieta, 2013).

2.2.3.6 Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA), según sus creadores es

> Una herramienta fácil de usar diseñada para los profesionales de TI que ayuda a las pequeñas y medianas empresas a determinar su estado de seguridad según las recomendaciones de seguridad de Microsoft y ofrece orientación de soluciones específicas. Mejore el proceso de administración de seguridad utilizando MBSA para detectar los errores más comunes de configuración de seguridad y actualizaciones de seguridad que falten en sus sistemas informáticos (Microsoft Corp, 2017).

MBSA es una herramienta de la compañía de *software* Microsoft, creadora de los sistemas operativos Windows. No es de código abierto, sin embargo es de distribución gratuita para usuario de los sistemas Windows. Como la Edificadora Beta cuenta con múltiples equipos corriendo Windows, se añade esta aplicación a la lista de herramientas a utilizar que no tienen costo para la empresa.

2.2.3.7 Oracle Virtual Box

Oracle describe su producto de virtualización como una herramienta que:

> Se puede usar tanto para empresas como para uso doméstico. VirtualBox no solo es un producto de gran rendimiento y alto rendimiento para los clientes empresariales, sino que también es la única solución profesional disponible gratuitamente como *software* de código abierto bajo los términos de la versión 2 de la GPL (GPL) (Oracle, s. f.).

En la actualidad, VirtualBox se ejecuta en Windows, Linux, Macintosh y Solaris y soporta un gran número de sistemas operativos invitados. Esta herramienta permitirá realizar pruebas de campo en la edificadora.

2.3 Definiciones y términos recomendados para la comprensión del documento

Es necesario definir ciertos términos que serán utilizados a lo largo del documento y facilitan su compresión. Para este efecto se extrajeron una serie de definiciones del glosario oficial de seguridad de (ISACA) creada para ayudar a los candidatos a sus certificaciones a entender las diferentes lecturas de seguridad en su documentación.

Aceptación del riesgo: si el riesgo está dentro de la tolerancia al riesgo de la empresa o si el costo de mitigar el riesgo es más alto que la pérdida potencial, la empresa puede asumir el riesgo y absorber cualquier pérdida

Activo: algo de valor tangible o intangible que vale la pena proteger, incluyendo a las personas, información, infraestructura, finanzas y reputación

Almacenamiento conectado a la red (NAS por sus siglas en inglés): forma de almacenamiento dedicado que centralizan el almacenamiento de datos.

Amenaza: cualquier cosa (por ejemplo, objeto, sustancia, humano) que sea capaz de actuar contra un activo de una manera que pueda resultar en daño.

Ataque: una ocurrencia real de un evento adverso.

Control: los medios de gestión del riesgo, incluidas las políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de carácter administrativo, técnico, de gestión o jurídico.

Confidencialidad: significa preservar las restricciones autorizadas en materia de acceso a la información y su divulgación, incluidos los medios para la protección de la privacidad y la propiedad de la información.

Cortafuegos: un sistema o combinación de sistemas que impone un límite entre dos o más redes, lo que forma típicamente una barrera entre un entorno seguro y abierto como Internet.

CVE: (Common Vulnerabilities and Exposure), siglas CVE, es una lista de información registrada sobre conocidas vulnerabilidades de seguridad, donde cada referencia tiene un número de identificación único.

Denegación de servicio: un asalto a un servicio de una sola fuente que lo inunda con tantas solicitudes que se sobresatura y se detiene completamente u opera a una tasa significativamente reducida.

Disponibilidad: significa garantizar el acceso oportuno y confiable y el uso de la información.

Hacker: una persona que intenta obtener acceso no autorizado a un sistema informático.

Impacto: magnitud de la pérdida resultante de una amenaza que explota una vulnerabilidad

Impacto, Análisis de: en un análisis de impacto, se identifican las amenazas a los activos y se determinan las posibles pérdidas empresariales para diferentes períodos de tiempo. Esta evaluación se utiliza para justificar el alcance de las salvaguardias que se requieren y los plazos de recuperación. Este análisis es la base para establecer la estrategia de recuperación.

Incidente, de seguridad: cualquier evento que no sea parte de la operación estándar de un servicio y que cause o pueda causar una interrupción o una reducción en la calidad de ese servicio.

Incidente, respuesta de: es la respuesta de una empresa a un desastre u otro evento significativo que pueda afectar significativamente a la empresa, su gente o su capacidad para funcionar productivamente. Una respuesta a un incidente puede incluir la evacuación de una instalación, iniciar un plan de recuperación de desastres (DRP) evaluación y cualquier otra medida necesaria para llevar a una empresa a un estatuto más estable.

Incidente, Plan de Respuesta: el componente operativo de la gestión de incidentes.

Integridad: significa protección contra la incorrecta modificación o destrucción de información y comprende la garantía de no repudio y autenticidad de la información.

Ransomware: *malware* que restringe el acceso a los sistemas comprometidos hasta que se satisfaga la demanda de rescate.

Riesgo: la combinación de la probabilidad de un evento y su consecuencia (ISO / CEI 73).

Riesgo, análisis de: es un proceso mediante el cual se estima la frecuencia y magnitud de los escenarios de riesgo de TI. Los pasos iniciales de la gestión de riesgos son analizar el valor de los activos para el negocio, identificar las amenazas a esos activos y evaluar la vulnerabilidad de cada activo a esas amenazas

Riesgo, apetito: la cantidad de riesgo, en un nivel amplio, que una entidad está dispuesta a aceptar en el cumplimiento de su misión.

Riesgo residual: el riesgo restante después de que la administración ha implementado una respuesta al riesgo.

Riesgo acumulado: el proceso de integración de las evaluaciones de riesgos a nivel corporativo para obtener una visión completa del riesgo general para la empresa.

Riesgo, tratamiento de: el proceso de selección e implementación de medidas para modificar el riesgo (ISO / IEC Guía 73, 2002).

Riesgo, transferencia de: el proceso de asignación de riesgo a otra empresa, generalmente a través de la compra de una póliza de seguro o mediante la subcontratación del servicio.

Vulnerabilidad: una debilidad en el diseño, implementación, operación o control interno de un proceso que podría exponer al sistema a amenazas adversas de eventos de amenaza.

Otros conceptos utilizados que se encuentran fuera del glosario de ISACA son:

MAC, dirección: dirección del *hardware* de control de acceso a soportes de un distribuidor que identifica los equipos, los servidores, los enrutadores u otros dispositivos de red. La dirección de control de acceso a soportes es un identificador único que está disponible en NIC y otros equipamientos de red. La mayoría de los protocolos de red usan IEEE: MAC-48, EUI-48 y EUI-64, que se diseñan para ser globalmente únicos. Un equipo en la red se puede identificar mediante sus direcciones MAC e IP. La dirección de control de acceso a soportes es un identificador único que está disponible en NIC y otros equipamientos de red (Symantec, s. f.).

Máquina Virtual: un contenedor de entorno o *software* que no existe físicamente, sino que se crea en otro entorno. Una máquina virtual puede ejecutar sus propios sistemas operativos y aplicaciones como si fuera un equipo físico (Symantec, s. f.).

BitLocker: es una característica de protección de datos que está disponible en Windows Server 2008 R2 superior y en algunas ediciones de Windows 7 o superior. La integración de BitLocker con el sistema operativo permite hacer frente a amenazas, por ejemplo, el robo de datos o la exposición en caso de pérdida, el robo o la retirada inapropiada de equipos. Los datos de un equipo que se ha perdido o ha sido robado pueden ser objeto de accesos no autorizados mediante la ejecución de una herramienta de ataque de *software* en el equipo o mediante la transferencia del disco duro a otro equipo. BitLocker

ayuda a mitigar el acceso no autorizado a datos porque mejora la protección del sistema y los archivos. Asimismo, BitLocker ayuda a hacer inaccesibles los datos cuando los equipos protegidos por esta característica se retiran o reciclan (Microsoft, s. f.).

Capítulo 3: Marco metodológico

3.1 Tipo de investigación

Con respecto a las metodologías a utilizar, se manifiesta que la investigación de tipo cualitativa es la más utilizada para el análisis de riesgos y cumple con los requisitos de ISO 27001, por tanto, es la base que se utilizó en este proyecto.

La investigación que se llevó a cabo es de tipo aplicada, basada en las tecnologías de código libre para la gestión de la ciber seguridad existentes en Costa Rica, por tanto no se requiere la formulación de una hipótesis.

Durante el desarrollo de esta investigación se describió de manera profunda las diferentes metodologías para la gestión de la ciber seguridad, sus aplicaciones prácticas, sus ventajas y desventajas, así como el tipo de gobierno que se debe de utilizar para proteger la información de los usuarios y de la compañía.

3.2 Alcance investigativo

El alcance investigativo de este documento combina las fases de exploración y descripción de los posibles riesgos que corre la empresa en cuestión durante la producción y manejo de su información, en donde se procederá a agrupar conocimiento para facilitar el cumplimiento de los objetivos de la empresa de una manera más segura y eficiente desde el punto de vista de análisis de riesgo, así como el establecimiento de los controles adecuados para mitigar dichos riesgos encontrados.

3.3 Enfoque

Como se mencionó con anterioridad, el enfoque apropiado y recomendado para este tipo de análisis es el cualitativo, este tiene como objetivo la descripción de las cualidades de un fenómeno. Busca un concepto que pueda abarcar una parte de la realidad. No se trata de probar o de medir en qué grado una cierta cualidad se encuentra en un cierto acontecimiento dado, sino de descubrir tantas cualidades como sea posible.

3.4 Diseño

El diseño para el estudio utilizado en este proyecto cualitativo se concentrará en dar en sentido y valor a los datos obtenidos en la fase de reconocimiento.

3.5 Población y muestreo

La población es el punto de partida para recolectar datos, para efectos de este proyecto, la población corresponde a los colaboradores de la Edificadora Beta, mientras que el muestreo, que en este caso es no probabilístico, busca conseguir una parte que sea suficientemente representativa de la población, para dar validez a los hallazgos que se obtuvieron mediante entrevista, observación y encuesta.

3.6 Instrumentos de recolección de datos

Hay que recordar que un instrumento de recolección de datos es cualquier recurso de que pueda valerse el investigador para acercarse a los eventos en estudio y extraer de información de ellos. Una vez definido el concepto, se procede a definir los instrumentos que se utilizaron para llevar a cabo la investigación:

Observación Participante: el autor de este documento generará conocimiento de cómo opera la empresa y los posibles riesgos a los cuales podrían estar expuesta mediante

una serie de visitas a las oficinas centrales, en donde se recolectarán datos de los procesos actuales, posibles riesgos en el manejo y almacenamiento de la información.

Entrevista: para obtener información sobre el estado actual de la empresa se procedió a conversar con el gerente general, los gerentes de las diferentes áreas, para así determinar los puntos de preocupación de cada uno de los departamentos de la empresa, así como las preocupaciones globales.

Entre las preguntas que prepararon para las entrevistas con los gerentes a guiar la conversación, se pueden mencionar algunas como:

1. ¿Tiene la empresa un manual de políticas documentadas?
2. ¿Conoce usted el término "gobierno corporativo" o gobernanza de TI?
3. ¿Se encuentran dichas políticas actualizadas y disponibles para todos los colaboradores?
4. ¿Contemplan dichas políticas como se debe de manipular la información de la empresa?
5. ¿Cuáles son los criterios que utiliza la empresa para evaluar al personal antes de contratarlo? ¿Verifican ustedes los antecedentes de los posibles futuros colaboradores?
6. ¿Han tenido algún tipo de brecha de seguridad en los últimos 2 años?
7. ¿Tienen algún tipo de clasificación de la información física y digital?
8. ¿Quién define el valor de la información en la empresa?

9. ¿Tiene la empresa entrenamientos en el área de seguridad de la información?
10. ¿Sabe usted qué es un análisis de riesgo?
11. ¿Sabe usted qué es Malware y que es lo que hace?
12. ¿Sabe qué es un “Cortafuegos” o “Firewall”, ¿tiene alguno instalado?
13. ¿Sabe qué es una brecha de seguridad?
14. ¿Se debe cumplir con alguna legislación o requisito específico de seguridad en su empresa?
15. ¿Tiene presupuesto asignado para la seguridad de la información en la empresa?
16. ¿En pocas palabras, que definiría usted como los puntos de dolor dentro de su empresa en lo que respecta a la seguridad de la información?

Cuestionario anónimo: para evaluar el conocimiento de los colaboradores de la empresa, se procedió a elaborar y aplicar un cuestionario corto que se detalla a continuación.

3.7 Técnicas de análisis de la información

Como referencia al por que debemos de definir las técnicas de análisis de información a utilizar en esta investigación podemos citar que:

> Las tecnologías de la información han experimentado crecimientos espectaculares desde los años 50, a un ritmo en el que la potencia de la informática crece exponencialmente todos los años. A este crecimiento natural de la informática le ha acompañado el de la información, cuyos volúmenes está haciendo que sea

indescifrable por sí sola. Esto ha obligado a los especialistas de esta rama a recurrir a sistemas de análisis para sacar su máximo valor.

Las empresas y entidades de información se dedicaban hasta hace poco más bien al almacenamiento de información para que los usuarios las utilizaran cuando y como pudieran. Ahora, con una visión más “agresiva”, los especialistas de información brindan no solo datos o grandes volúmenes de información, sino que entregan informes, producto de análisis, con los cuáles les ayudan a convertir tantos datos en información sintetizada y confiable. Estos análisis de información ayudan a la toma de decisiones, que es una tarea que se hace cada vez más dinámica y requiere de un basamento informativo bien sustentado (Sarduy Domínguez, 2007, s. p.).

Capítulo 4: Análisis del diagnóstico

4.1 Plan de trabajo

A continuación, muestra una tabla que contiene la lista de actividades a realizar durante la fase de exploración en la empresa para determinar sus necesidades en lo que respecta a la protección de la información.

Actividad	Responsable	Tiempo	Recurso	Estatus
Obtener autorización y apoyo de la gerencia para la elaboración del proyecto	Roberto.	2 semanas.	Gerencia	Completo
Aceptación de la carta de intención preparada por Roberto para la gerencia.	Roberto.	1 día.	Gerencia	Completo
Coordinación y establecimiento de las visitas a San Carlos.	Roberto.	1 día.	Gerencia, Eduardo, Roberto.	
Asignación de un recurso de la edificadora para asistir en la gestión del proyecto. Asignado. Sr Eduardo Mora de TI.	Roberto.	2 semanas.	Eduardo Mora	Completo
Exploración y verificación de la seguridad física en las instalaciones de la empresa.	Roberto.	1 día.	Roberto y Eduardo	Completo
Exploración del centro de datos de la empresa.	Roberto.	1 día.	Roberto y Eduardo	Completo
Entrevista con los gerentes de los diferentes departamentos.	Roberto.	1 día.	Gerencia y Roberto	Completo
Aplicación de los cuestionarios para los gerentes.	Roberto.	1 día.	Gerencia y Roberto	Completo
Conseguir organigrama de la empresa.	Roberto.	1 semana.	Gerencia	Completo
Conseguir las políticas de la empresa	Roberto.	1 semana.	Gerencia	Completo
Listado de los activos de la empresa	Roberto.	3 días.	Roberto y Eduardo	Completo
Correr los escáneres para la detección de activos y de vulnerabilidades en estos.	Roberto.	1 día.	Roberto y Eduardo	Completo
Aplicar el cuestionario de seguridad física	Roberto.	2 días.	Roberto	Completo.
Aplicar encuestas al personal para verificar su conocimiento de seguridad	Roberto.	1 día.	Roberto y colaboradores de Beta	Completo.
Tabulación de los datos de las encuestas y generación de los resultados.	Roberto.	2 días.	Roberto	Completo.
Con la información recopilada, realizar un análisis de riesgo.	Roberto.	4 semanas.	Roberto.	Completo.

Documentar adecuadamente los hallazgos y determinar cuáles controles pueden ser implementados primero a corto plazo y cuales deben de tratarse a mediano o largo plazo.	Roberto.	4 semanas.	Roberto.	Completo.
Crear las guías de implementación de los controles sugeridos por el análisis de riesgo basado en los recursos existentes.	Roberto.	6 semanas.	Roberto.	Completo.
Presentación de los resultados a la gerencia	Roberto.	1 día.	Roberto.	Completo.
Preparación de la implementación de las herramientas de código abierto a implementar en la edificadora.	Roberto.	2 semanas.	Roberto	Completo
Instalación de la herramienta para la gestión de claves en cada una de las estaciones de trabajo	Eduardo.	1 semana.	Eduardo	Completo.
Entrenamiento del personal en la herramienta de gestión de claves.	Roberto y Eduardo.	1 día.	Roberto y Eduardo.	Completo.
Instalación del servidor de archivos utilizando la solución de FreeNAS	Roberto y Eduardo.	2 días.	Roberto y Eduardo.	Completo.
Instalación del servidor proxy basado en SQUID	Roberto y Eduardo.	2 días.	Roberto y Eduardo	Completo.
Presentación de los documentos de entrenamiento sobre temas de seguridad para los colaboradores de Beta	Roberto.	1 día.	Roberto	Completo.

Tabla 1 Listado general de actividades a realizar durante el desarrollo del proyecto.

Fuente: Elaboración propia.

4.2 Pasos a seguir para realizar una adecuada gestión de riesgos

Siguiendo como base las buenas prácticas recomendadas por la metodología MAGERIT para efectuar un análisis de riesgo efectivo, se realizaron las siguientes actividades basados en los pasos recomendados en dicha metodología.

1. Identificación de los activos importantes para la compañía, su interrelación y su valor, en el sentido en que afectaría su degradación o pérdida.
2. Determinar y enumerar a que amenazas están expuestos los activos identificados durante el proceso anterior.

3. Establecer que medidas preventivas o controles existen y que tan eficientes son para el manejo del riesgo encontrado.

4. Medir el impacto causado a la organización en caso de que el activo sufra de una materialización de una amenaza.

5. Medir el riesgo residual luego de la aplicación de los controles.

Cabe recordar que la gestión de riesgos en un proceso cíclico que debe de adoptarse como parte de los procesos principales de la empresa, esto es que cada cierto tiempo el análisis debe de repetirse para verificar si existen nuevos activos, si los controles existentes aún cumplen con su objetivo y que controles se han vuelto obsoletos con el tiempo y ya requieren actualización.

4.2.1 Identificación de los activos importantes para la compañía

En este paso se procede a identificar los activos que correspondan a un componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para el funcionamiento normal de la edificadora.

En esta enumeración pueden incluirse activos tales como: información, datos, servicios, aplicaciones informáticas, equipos computacionales, comunicaciones, recursos administrativos, recursos físicos y por supuesto el más importante, el factor humano.

4.2.1.1 Enumeración de los activos computacionales de la empresa

Para efectos de la valoración de los activos correspondientes a equipos computacionales, se procedió a visitar al departamento de contabilidad para obtener información sobre los equipos comprados en la empresa y su valor actual. Dicha

información la empresa la maneja mediante documentos de Excel guardados en la computadora del encargado de contabilidad, con respaldos en el servidor de archivos principal. La hoja de Excel mencionada cuenta con los siguientes campos de información debidamente llenos.

Rubro	Descripción del rubro
COD	Corresponde al identificador único de cada activo
CODIGODEP	Corresponde al código de departamento dueño del equipo
DESCRIPCION	Descripción breve del equipo con sus especificaciones y modelo
SERIE	Número de serie del activo
FECHA	Fecha de compra del activo
RESPONSABLE ASIGNADO	Nombre de la persona que esta activamente usando el activo y es el responsable de este.
NOTAS	Notas generales como "se le cambio el disco duro", etc.
VALORORIGINAL	Valor origina del activo según factura comercial
VIDAUTIL	Tiempo en meses que define en cuanto tiempo se depreciará el activo - 60 meses para equipo de cómputo
DEPREMENSUAL	Monto de depreciación mensual del activo
VALOR EN LIBROS	Valor original - depreciación acumulada
DEPREACUM	Sumatoria de la depreciación mensual

Tabla 2 Encabezados de la hoja de Excel de contabilidad para enumerar los activos.

Fuente: Edificadora Beta y Roberto Buján

Durante una de las conversaciones con el encargado de TI, se determinó que existe una copia extra oficial de los activos que maneja dicho encargado, en donde se agrega información adicional como los componentes que se le han cambiado a los equipos (reparaciones), así como a fecha de estos cambios. Existe una consciencia de que los

activos debe de llevarse controlados a nivel contable, pero no a nivel de TI, por ejemplo, la empresa no sería capaz de identificar un equipo conectado a la red que no fuera de su propiedad, debido a que no tienen un listado de las direcciones MAC de las tarjetas de red de los equipos.

Como buena práctica, la edificadora debe de llevar a cabo un inventario de equipo de cómputo, *software* y mobiliario, para determinar cuál es la información crítica que se tiene que resguardar, adicionalmente levantar un inventario de los servicios de cómputo, telecomunicaciones, internet, etc., que son requeridos para que los usuarios puedan llevar a cabo sus actividades normales. En el caso de la constructora, para efectos de este proyecto se requiere un inventario de activos de tecnologías de información y aquellos activos que estén relacionados directamente a estos.

Para efectos de este proyecto, la gerencia manifestó su preocupación de que información sensitiva de la empresa que pudiera utilizarse para efectos de vulnerar la seguridad de la empresa se mostrara en este escrito, por tanto se procedió a reemplazar los datos de algunas tablas y gráficas con datos ficticios para su protección, como por ejemplo los rangos reales de los IPs, las direcciones MAC de los equipos, las versiones de sistemas operativos reales corriendo en la constructora, etc., dichos datos no afectan la lectura del documento por tanto, no se considera necesario el presentar la información real.

4.2.1.1.1 Listado de activos - Servidores

Tanto los servidores como la información contenida y los servicios que prestan se consideran activos esenciales, por tanto ambos debe de ser enumerados dentro del documento de control. Para efectos de control de esta información y al número de equipos,

se puede utilizar una hoja de excel para llevar el control, debido a que los cambios en la cantidad de los equipos no cambia con frecuencia.

La hoja usada para enumerar los activos tomó como base la hoja que ya estaba utilizando el personal de manera informal para llevar un control similar al deseado, así que se procedió a agregar campos adicionales para poder llevar una bitacora de los equipos de manera separada de los otros activos de la empresa.

Código Activo	Modelo del Equipo	Año de Compra	Funcion	IP Asignado	Sistema Operativo	Costo	MAC Address
A-1-00001	PowerEdge R320	2012	Active Directory / DNS bind v9	192.168.0.50	Windows Server 2012 R2	$4,000	12-B2-ED-25-0B-27
A-1-00002	PowerEdge R320	2013	Servidor de Archivos / SMB V3	192.168.0.51	FREENAS 9.10	$4,000	F5-0C-96-D0-E7-37
A-1-00003	PowerEdge R320	2013	Proxy Server - SQUID 3.5.25	192.168.2.10	Ubuntu Server 14.04 LTS	$4,000	96-AE-27-FC-AB-54
A-1-00004	PowerEdge R320	2013	DNS Server - BIND9	192.168.2.11	Ubuntu Server 14.04 LTS	$4,000	78-23-6C-69-1B-0E

Figura 11 Formato propuesto para el control de los servidores.

Fuente: Elaboración propia.

4.2.1.1.2 Listado de activos - Estaciones de trabajo.

Las estaciones de trabajo se consideran activos auxiliares, ya que si se pierden o se dañan algunas de ellas la operación puede continuar, en forma degradada, pero puede seguir. Sin embargo, la pérdida de dos o más equipos puede impactar la operación al quedar colaboradores sin equipos. Normalmente se mantienen algunos equipos usados algo viejos que se pueden usar como medida de contingencia mientras se repara o cambia los equipos dañados. Las buenas prácticas recomiendan que la información contenida en estos equipos debería de estar respaldada en el servidor de archivos, de hecho la gerencia recomienda a los colaboradores que hagan el respectivo respaldo, sin embargo se dan casos en donde los

colaboradores ignoran dichas recomendaciones y sencillamente no tienen ninguna política que los obligue a hacerlo.

Con el inventario de las estaciones de trabajo, se debería de considerar el hecho de que es indispensable llevar un inventario riguroso de estos equipos, pues en muchos casos contienen las propuestas, diagramas, planos y otro tipo de propiedad intelectual de la edificadora y constituye un activo de alto valor para la empresa, por tanto, si se detecta que faltan equipos, debe de reportarse inmediatamente, Asimismo, si en la red aparecen equipos que no se encuentran en la lista, podría ser que existe un equipo no autorizado y se deberá proceder con su búsqueda, de allí la importancia de tener los equipos bien inventariados.

Código de Activo	Nombre del activo	ID del Usuario Asignado	Sistema Operativo	Costo Aproximado	Mac Adr
A-2-00221	usuario_mobl1	1230750001	Windows 10 v1607	$1,500	F9:89:41:1F:BC:B7
A-2-00222	usuario_mobl2	1230750002	Windows 10 v1607	$1,500	44:A0:F2:B8:63:BB
A-2-00223	usuario_mobl3	1230750003	Windows 10 v1607	$1,500	75:76:8F:20:C4:23
A-2-00224	usuario_mobl4	1230750004	Windows 10 v1607	$1,500	93:F7:1E:98:AA:2B
A-2-00225	usuario_mobl5	1230750005	Windows 10 v1607	$1,500	E4:62:97:38:97:E1
A-2-00226	usuario_mobl6	1230750006	Windows 10 v1501	$1,500	9E:4D:05:95:A4:1D
A-2-00227	usuario_mobl7	1230750007	Windows 10 v1501	$1,500	DB:DB:DB:F1:D1:3F
A-2-00228	usuario_mobl8	1230750008	Windows 10 v1501	$1,500	CD:7F:7F:1A:6A:4F
A-2-00229	usuario_mobl9	1230750009	Windows 10 v1501	$1,500	7E:41:EB:9B:F4:04
A-2-00230	usuario_mobl10	1230750010	Windows 10 v1501	$1,500	3E:5C:D1:0C:17:BD
A-2-00231	usuario_mobl11	1230750011	Windows 10 v1501	$1,500	53:9C:09:3A:EA:A7
A-2-00232	usuario_mobl12	1230750012	Windows 10 v1607	$1,500	24:C7:BA:0E:BE:1B
A-2-00233	usuario_mobl13	1230750013	Windows 10 v1607	$1,500	88:B2:A2:2F:9B:B0
A-2-00234	usuario_mobl14	1230750014	Windows 10 v1607	$1,500	36:2D:5A:F1:F7:DE
A-2-00235	usuario_mobl15	1230750015	Windows 10 v1607	$1,500	C9:04:B0:0D:B6:32
A-2-00236	Ingenieria_WS1	1230750016	Windows 10 v1420	$2,500	15:59:68:46:34:CF
A-2-00237	Ingenieria_WS2	1230750017	Windows 10 v1420	$2,500	9F:97:9A:E1:4D:C2
A-2-00238	Ingenieria_WS3	1230750018	Windows 10 v1420	$2,500	48:03:CD:66:A5:63
A-2-00239	Ingenieria_WS4	1230750019	Windows 10 v1420	$2,500	02:81:BA:AF:9E:E8
A-2-00240	Ingenieria_WS5	1230750020	Windows 10 v1420	$2,500	C5:4F:BB:A4:90:1A

Figura 12 Formato propuesto para el listado de estaciones de trabajo: Fuente: Elaboración propia.

4.2.1.1.3 Listado de activos - Equipos de Red

Los equipos de red, debido al servicio que prestan, se consideran activos esenciales y en caso que algo los comprometa, puede causar una degradación o incluso una denegación del servicio, impactando económicamente a la edificadora. Asimismo, llevar el control de la versión de *software* que está corriendo cada uno de los equipos es importante, debido a que, pudiera existir una actualización crítica pendiente en un equipo que arregla una vulnerabilidad que permitiría un ataque remoto, por ejemplo. Por tanto, si se tiene inventariado la versión del sistema operativo o firmware, se podrá parchar el equipo a tiempo, antes de que este sea atacado.

Adicionalmente, mediante el uso de escáneres de vulnerabilidades es posible determinar cuáles equipos son vulnerables y lo seguirán siendo, debido a que el equipo podría estar fuera de la ventana de soporte del mismo.

No de Serie	Modelo Equipo	Funcion	IP estáticos.	Dirección MAC	Sistema Operativo	Versión	Vulnerabl	Costo
A-3-00001	DSL-7740C - KOLBI VDSL (ADSL3)	MODEM VDSL3	* 201.202.18.36/22 * 192.168.0.1/24	AA:97:B1:A9:F4:DF - 4A:1F:20:46:DA:D2	Firmware personalizado Kc	1.0b	No	$200.00
A-3-00002	ZyXEL 24-Port Gigabit Ethernet Smart Managed Rackmount Switch	Network Switch	* 192.168.0.25/24	75:92:FA:E3:8A:13	ZyXEL default firmware	1.5c	No	$450.00
A-3-00003	HP LaserJet Pro M227fdw All-in-One Wireless Laser Printer (G3Q75A).	Impresora	* 192.168.0.30/24	E9:F4:03:E9:41:89	HP Firmware	v1.85	No	$6,000.00
A-3-00004	HP LaserJet Pro M227fdw All-in-One Wireless Laser Printer (G3Q75A).	Impresora	* 192.168.0.31/24	1D:B5:88:FF:C9:9E	HP Firmware	v1.85	No	$6,000.00
A-3-00005	Linksys AC5400 Tri Band Wire	Wireless	* 192.168.0.40/24	19:F9:FF:01:09:8D	Linksys Router Firmware	v1.1	No	$400.00

Figura 13 Formato propuesto para el listado del equipo de red básico.

Fuente: Elaboración propia.

4.2.1.1.4 Dependencias existentes entre los activos identificados.

Para determinar las dependencias entre los activos fue necesario clasificarlos de acuerdo a la función que cumplen en la empresa. Según la metodología MAGERIT, se deben de extraer las siguientes características de los activos:

a. Los datos a los que se tiene acceso.

b. Las aplicaciones que manejan

c. Los equipos informáticos que gestiona

d. Los servicios que gestiona.

ID del Recurso	Nombre del recurso	Descripción
1	Servidor de Dominio	Servicio de red
2	Servidor de Archivos	Servicio de red
3	Acceso a Internet	Servicio de red
4	Civil CAD	Software de diseño
5	SAP	Sistema contable
6	Midas design 2014	Software de ingeniería
7	Licencia ptc mathacad prime	Software de ingeniería
8	Licencias para presto 2015.	Software de ingeniería
9	Servicios de correo electrónico.	Servicio de red
10	Servicios de VPN / Acceso remoto	Servicio de red
11	Estaciones de trabajo	Consumidor de servicios
12	Documentos Beta.	Información generada para los proyectos.

Tabla 3 Listado de los recursos asociados a los activos.

Fuente: Elaboración propia.

Estaciones de Trabajo	Depende de (recurso)	Ofrece (recurso)
usuario_mobl1	1,2,3,9,10	4,12
usuario_mobl2	1,2,3,9,10	4,12
usuario_mobl3	1,2,3,9,10	4,12
usuario_mobl4	1,2,3,9	5,12
usuario_mobl5	1,2,3,9	5,12
usuario_mobl6	1,2,3,9	5,12
usuario_mobl7	1,2,3,9	6,12
usuario_mobl8	1,2,3,9	6,12
usuario_mobl9	1,2,3,9	7,12
usuario_mobl10	1,2,3,9	8,12
usuario_mobl11	1,2,3,9	8,12
usuario_mobl12	1,2,3,9	8,12
usuario_mobl13	1,2,3,9	1,12
usuario_mobl14	1,2,3,9	1,12
usuario_mobl15	1,2,3,9	1,12
usuario_WS1	1,2,3,9	1,12
usuario_WS2	1,2,3,9	1,12
usuario_WS3	1,2,3,9	1,12
usuario_WS4	1,2,3,9	1,12
usuario_WS5	1,2,3,9	1,12

Tabla 4 Dependencias de recursos de las estaciones de trabajo de la edificadora.

Fuente: Elaboración propia

Nótese que el 100 % de las estaciones de trabajo dependen directamente de los recursos 1,2,3 y 9. Adicionalmente el recurso 12, que corresponde a la información generada por los colaboradores en sus estaciones de trabajo, representa mucho volumen en lo que respecta a los recursos. Este hay que tomarlo en consideración a la hora de considerar una posible degradación del servicio debido al impacto en estos activos.

4.2.1.1.5 Valoración de los activos basado en su criticidad.

Para valorar los activos, se tomarán los siguientes conceptos de seguridad de la información.

D Disponibilidad de los datos

I Integridad de los datos.

C Confidencialidad de los datos.

Valor			Criterio
10	Muy Alto	MA	Daño muy grave a la edificadora
7-9	Alto	A	Daño grave a la edificadora
4-6	Medio	M	Daño importante a la edificadora
1-3	Bajo	B	Daño menor a la edificadora
0	Despreciable	D	Daño irrelevante a la edificadora

Tabla 5 Escala de impacto.

Fuente: elaboración propia

ID	Nombre del recurso	D	I	C
1	Servidor de Dominio	5	8	5
2	Servidor de Archivos	7	8	8
3	Acceso a Internet	7	7	5
4	Civil CAD	1	1	1
5	SAP	5	10	10
6	Midas design 2014	3	3	3
7	PTC mathacad prime	2	2	2
8	Presto 2015.	2	2	2
9	Servicios de correo electrónico.	6	8	9
10	Servicios de VPN / Acceso remoto	3	3	6
11	Estaciones de trabajo.	5	5	6
12	Información generada para los proyectos.	9	9	10

Tabla 6 Listo de recursos informáticos.

4.2.1.2 Valoración de la seguridad física de la edificadora Beta

Debido a que la información se almacena de manera física, así como digital, la seguridad de la integridad física de los documentos y los medios de almacenamiento también deben considerarse, por tanto, un estudio sobre la seguridad física a las instalaciones de la Edificadora Beta es necesario para poder garantizar que se están tomando las medidas adecuadas para proteger la información de la empresa.

Para lograr determinar el estado de la seguridad física, se procedió a aplicar el cuestionario "*Lista de verificación de la seguridad física*" que se encuentra disponible en

los anexos, en donde se fueron evaluando cada uno de los factores de riesgo que podrían afectar la integridad de los activos y por ende, su información contenida.

Grupos Evaluados	Resultado Evaluación - Riesgo
Barreras Del Perímetro – Instalaciones	(1-3) Bajo
Iluminación Para Protección	(1-3) Bajo
Alarmas De Protección	(1-3) Bajo

Tabla 7 Resultados del análisis de la seguridad física.

Fuente: elaboración propia basados en el cuestionario de seguridad física disponibles en los anexos.

A pesar de que la edificadora ha contado con asesoramiento formal sobre la seguridad física, en términos generales, se califica su condición actual como aceptable, no se encontró ningún hallazgo crítico que pudiera comprometer los activos alojados dentro del edificio.

4.2.2 Determinar y enumerar a que amenazas están expuestos los activos identificados durante el proceso anterior

Siguiendo los conceptos mencionados en la metodología MAGERIT (y casi que en cualquier metodología de análisis de riesgos), al determinar la amenaza que afecta negativamente a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos: **degradación**, es decir conocer cuán afectado estaría el activo y por la **probabilidad**, es decir que tan probable o improbable es que se materialice la amenaza.

4.2.2.1 Enumeración de los hallazgos encontrados durante el reconocimiento

A continuación, se describen una serie de hallazgos que fueron resultado de la observación directa, las encuestas y cuestionarios, así como el trabajo de campo.

- Hallazgo 1: luego de aplicar las encuestas, se determinó que los usuarios en general, no tienen un conocimiento adecuado en temas de seguridad de claves y cuidados a la hora de bloquear los equipos cuando se alejan de estos.

- Hallazgo 2: en conversaciones con la gerencia, ellos comentaron sobre incidentes que han ocurrido en donde colaboradores de la empresa han caído en los correos de *phishing* buscando usuarios del Banco Nacional de Costa Rica y como sus cuentas se han visto comprometidas en varias ocasiones debido a este hecho.

- Hallazgo 3: se detectó la ausencia de escritorio limpio en algunas estaciones de trabajo, en donde se guardan claves debajo del teclado para evitar olvidos.

- Hallazgo 4: mediante el escáner de vulnerabilidades, se detectaron una serie de sistemas que no están al día con los parches de seguridad.

- Hallazgo 5: la mayoría de los colaboradores de la empresa generan contenido mediante la elaboración de estudios, diagramas y planos de los proyectos en los que trabajará la empresa. El problema radica en que no existe consistencia en donde se guardan los datos, mientras algunos trabajan y respaldan en el servidor de archivos, hay otros que trabajan con los archivos locales. Por tanto, si el sistema falla, sufre un robo o es infectado con *malware*, los datos corren el riesgo de perderse.

- Hallazgo 6: se logró identificar 31 perfiles en la red social de profesionales Linkedin relacionados con la Edificadora Beta. Sin embargo, no fue posible localizar una política u entrenamiento en donde se eduque a los usuarios sobre qué clase de información de proyectos de Beta pueden compartir en esta red.

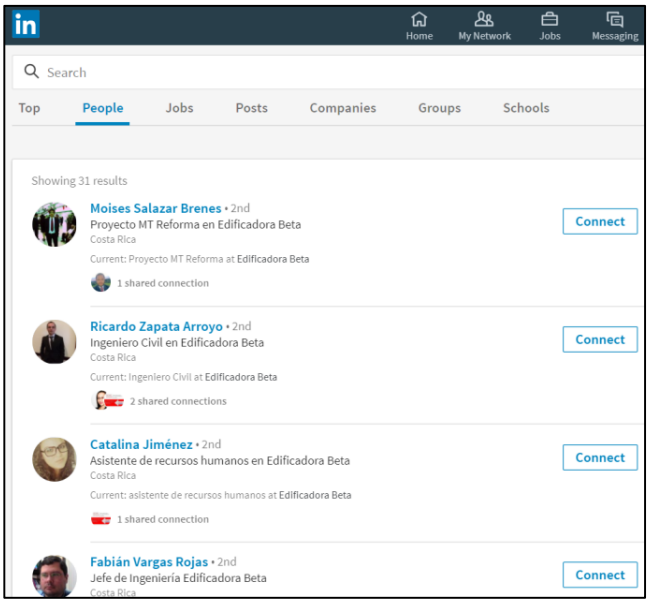


Figura 14 Perfiles asociados a la edificadora Beta en la red Linkedin.

Fuente: red social Linkedin

Hallazgo 7: observando el cuarto de telecomunicaciones y luego de confirmar las observaciones, se llegó a la conclusión de que a pesar de la alta dependencia que tienen las operaciones de día a día de la edificadora, no cuentan con un enlace redundante que les permita seguir operando, aunque sea de forma degradada en caso de que el enlace principal caiga. Como la edificadora trabaja en el campo de licitaciones, la entrega tardía de una de

estas licitaciones podría implicar la pérdida de un concurso y por ende, un impacto importante al negocio.

Hallazgo 8: Se detectaron puertos no utilizados abiertos y sin supervisión. En el caso de estaciones de trabajo de los colaboradores de la empresa, una máquina podría estar infectada y estar enviando virus tanto dentro como fuera de la red sin saberlo. En el caso de los servidores que tienen acceso directo a internet a través de una IP pública, tener dichos puertos abiertos facilita a un atacante externo un ataque directo al activo.

Hallazgo 9: router no bota las conexiones abiertas incompletas, lo que da como resultado que este sea vulnerable a un ataque de denegación de servicio. Esto es, en caso de que un competidor de Beta quisiera que estos no participen en una licitación, podrían contratar a un atacante para que bote la conexión a internet mediante un ataque directo a esta vulnerabilidad.

Hallazgo 10: las claves del enrutador inalámbrico no se cambian de manera regular, lo que facilita la entrada de un intruso a dicha red mediante el uso de herramientas de hackeo para redes inalámbricas.

Hallazgo 11: falta de controles físicos para conectar equipo a los puntos de red en el edificio, con esto es posible conectar dispositivos no homologados (que podrían estar infectados por virus) a la red interna, lo que permitiría actividades tales como descarga de contenido ilegal como películas y juegos e incluso, copias no autorizadas de los datos de la empresa.

Hallazgo 12: luego de la entrevista con la gerencia, se detectó la ausencia de controles y procesos para la separación de empleados. No existe un proceso en el que se

describa el paso a paso de actividades que se deben de seguir cuando es necesario separar a un colaborador de la empresa, ya sea por retiro, renuncia o despido.

Hallazgo 13: solución antivirus no detecta ataque de día cero, recayendo en los colaboradores de la empresa la responsabilidad de escoger que archivos abren de internet y cuáles no. Sin embargo, los colaboradores no reciben una capacitación formal en este campo, por lo que ellos son el eslabón más débil en la cadena de seguridad de la información de la empresa.

Hallazgo 14: a nivel del servidor, se encontró un servidor de archivos de archivos basado en Linux, distribución Mint versión 17.3, la cual cuenta con actualizaciones de *software* garantizadas hasta abril del 2019. Dicho servidor cuenta con varios discos para el respaldo de datos. Sin embargo, no se encuentra configurado en espejo para proteger los datos en caso de un fallo de disco.

Hallazgo 15: la gerencia manifestó su preocupación sobre el hecho de que sus colaboradores puedan tener el correo electrónico de la empresa configurado en el teléfono y de cómo ellos sienten que no tienen el control sobre los datos alojados allí, ya que ellos utilizan la solución de Google para empresas. Sin embargo, luego de conversar con el encargado de TI, se llegó a la conclusión de que existen las herramientas para enviar políticas de seguridad desde la consola de administración de Google, sin embargo estas políticas no están implementadas.

4.2.2.2 Elaboración de tablas para determinar las amenazas y vulnerabilidades asociadas a cada activo

Basado en la información obtenida y documentada en los hallazgos, se procedió a la elaboración de tablas para determinar las amenazas y vulnerabilidades asociadas a cada activo, así como el impacto asociado en caso de que se dé un evento de seguridad.

ID Activo	Amenaza	Vulnerabilidad	Impacto
12	Hacker, otro colaborador de la empresa.	Usuarios no entrenados vulnerables a ingeniería social.	Acceso inapropiado a los sistemas y archivos de la empresa. Robo de Información.
12	Hacker a través de phishing	Usuario no entrenado en temas te seguridad de correo electrónico.	Robo/pérdida de Información
12	Hacker / atacante interno.	Políticas deficientes - Claves de usuario sin la adecuada protección - Ausencia de escritorio limpio	Robo de Información.
1,2,11,12	Hacker a través de malware / atacante externo.	Sistemas vulnerables.	Infección de equipos/Pérdida de información/Baja productividad por equipos degradados.
11,12	Hacker a través de malware, Ladrón a través de hurto del activo.	Gestión de respaldos no consistente, falta de políticas de seguridad con respecto al uso del material electrónico de la empresa.	Pérdida de información valiosa para la empresa por fallo, robo o infección.
12	Usuario interno no entrenado.	Usuario no entrenado para no compartir información en redes sociales	Un usuario no entrenado pudiera divulgar información importante que represente ventaja competitiva por compartir información en redes sociales de trabajo como LinkedIn.
3,9,10	Fallo infraestructura.	Ausencia de conexión redundante	Como se determinó en el evalúo de los recursos requeridos para funcionar, un fallo en el internet deja a la empresa inactiva mientras el servicio se restaura, implicando impacto económico.
2,10,12	Hacker.	Puertos no utilizados abiertos y sin supervisión	Puertos abiertos no utilizados ni monitoreados representa una puerta de acceso para un atacante remoto en caso de que este localice un sistema vulnerable.
3,9,10	Hacker mediante ataque remoto.	Router no bota las conexiones abiertas incompletas	El router actual, al no estar debidamente configurado, es vulnerable a ataques sencillos de denegación de servicio.
3,9,10	Hacker.	Claves del enrutador inalámbrico no se cambian de manera regular. Al tener la misma clave siempre, esta puede ser obtenida mediante ataques de fuerza bruta.	Denegación del servicio de red inalámbrico.

3, 9,10,12	Usuario interno.	Falta de controles físicos para conectar equipo a los puntos de red en el edificio.	Un usuario podría conectar a la red un equipo que no sea propiedad de la empresa. Pudiendo cometer actos como hurto de información o incluso usar la conexión de internet para bajar material ilegal (películas, juegos, etc.), disminuyendo el ancho de banda disponible y exponiendo a la empresa a problemas legales.
1,2,3,5,11,12	Usuario interno.	Falta de controles y procesos para la separación de empleados.	Un empleado descontento que sospecha que lo van a liquidar, podría robar información de la empresa o sabotear algún sistema.
11,12	Hacker mediante Malware – Ransomware.	Solución antivirus no detecta ataque de día cero, recayendo en los colaboradores de la empresa la responsabilidad de escoger que archivos abren de internet y cuáles no.	Un malware dentro de la red puede cifrar todos los documentos alojados en los equipos de la empresa, causando pérdidas importantes de información.
2,12	Fallo de *hardware* en el equipo.	Servidor no configurado en espejo para proteger la información. Sistema de archivos con mediana tolerancia a corrupción de datos.	El servidor de archivos no cuenta con una configuración de espejo, por tanto, es vulnerable a un fallo físico de disco.
12	Ladrón.	Robo de teléfono celular con información de la edificadora en él	Información confidencial puede filtrarse perdiendo ventaja competitiva.

Tabla 8 Identificación de las amenazas, las vulnerabilidades sobre los activos y el impacto generado.

Fuente: Elaboración propia

4.2.2.3 Cálculo del riesgo total calculado sobre la probabilidad e Impacto

A continuación, se presenta la tabla de riesgo total calculado sobre la probabilidad e Impacto, se utiliza una escala de colores: verde denota valores bajos, amarillo valores medios y rojo valores altos o críticos. El valor 1 es el más bajo y 5 el más alto.

NOTA: El riesgo se determina por la multiplicación de la probabilidad por el impacto. Por ejemplo, si un evento tiene una probabilidad de 5 (Altamente probable) y un impacto de 5 (catastrófico), el riesgo sería 25, el cual es el valor máximo.

ID Activo	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo Total
12	Hacker, otro colaborador de la empresa.	Usuarios no entrenados vulnerables a ingeniería social.	2	5	10
12	Hacker a través de phishing	Usuario no entrenado en temas te seguridad de correo electrónico.	5	5	25
	Hacker / atacante interno.	Políticas deficientes - Claves de usuario sin la adecuada protección - Ausencia de escritorio limpio	4	4	16
1,2,11 y 12	Hacker a través de malware / atacante externo.	Sistemas vulnerables.	4	4	16
11 y 12	Hacker a través de malware, Ladrón a través de hurto del activo.	Gestión de respaldos no consistente, falta de políticas de seguridad con respecto al uso del material electrónico de la empresa.	3	5	15
12	Usuario interno no entrenado	Usuario no entrenado para no compartir información en redes sociales	3	4	12
3,9 y 10	Fallo infraestructura	Ausencia de conexión redundante	2	4	8
2,10,12	Hacker	Puertos no utilizados abiertos y sin supervisión	3	5	15
3,9,10	Hacker mediante ataque remoto	Router no bota las conexiones abiertas incompletas	3	4	12
3,9,10	Hacker	Claves del enrutador inalámbrico no se cambian de manera regular. Al tener la misma clave siempre, esta puede ser obtenida mediante ataques de fuerza bruta. Adicionalmente, al ser una clave vieja, existe la posibilidad que mucha gente la conozca	2	2	4
3, 9,10,12	Usuario interno	Falta de controles físicos para conectar equipo a los puntos de red en el edificio.	3	4	12
1,2,3,5,11,12	Usuario interno	Falta de controles y procesos para la separación de empleados.	2	4	8
11,12	Hacker	Solución antivirus no detecta ataque de día cero, recayendo en los colaboradores de la empresa la responsabilidad de escoger que archivos abren de internet y cuáles no.	3	5	15

2,12	Fallo de hardware.	Servidor no configurado en espejo para proteger la información. Sistema de archivos con mediana tolerancia a corrupción de datos.	2	5	10
12	Ladrón.	Robo de teléfono celular con información de la edificadora en él	2	5	10

Tabla 9 Riesgo total calculado sobre la probabilidad e Impacto.

Fuente: Elaboración propia.

Luego de analizar las tablas de resultados, es evidente que el activo más afectado por las amenazas es la información de la empresa y de como esta se puede perder por la ausencia de controles en diversas áreas.

4.2.3 Establecer que medidas preventivas o controles existen y qué tan eficientes son para el manejo del riesgo encontrado

Vale la pena recordar que los controles son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo, por tanto sus implementaciones ayudarán a controlar las amenazas que pudieran afectar los activos de la edificadora.

En la siguiente tabla, se detallan una serie de controles creados para mitigar las amenazas asociadas a los activos en forma de recomendaciones generales.

ID del hallazgo	Amenaza	ID Activo	Control
1	Hacker, otro colaborador de la empresa.	12	Se deben de crear una serie de documentos para los entrenamientos en donde se les enseñe a los usuarios que es ingeniería social y como se puede causar daño a la empresa usando las claves de otra persona para no ser detectados.
2	Hacker a través de phishing	12	Se deben de crear una serie de documentos y entrenamientos en donde se les enseñe a los usuarios que sobre los diferentes tipos de ataques por medio de correo electrónico para lograr obtener información de cuentas bancarias. Montaje de un servidor de proxy que realice tareas de filtrado de sitios web, para ayudar a proteger a los usuarios de direcciones web con código malicioso. Para esta solución, se puede utilizar un servidor proxy de código

			abierto basado en SQUID.
3	Hacker / atacante interno.	12	Utilizar las áreas cerradas, protección de los dispositivos y sistemas de información, restricciones a la hora de utilizar la copia y la impresión de tecnología, adoptar una cultura sin papel. Uso de una solución de código abierto para la gestión de claves, como por ejemplo KeePass,
4	Hacker a través de malware / atacante externo.	1,2,11,12	Instalación de un escáner de vulnerabilidades. Pueden utilizarse soluciones tales como las contenidas en la distribución de Linux para pruebas de penetración Kali Linux, así como el "Microsoft Baseline Security Analyzer" de Microsoft. Montaje de un sistema de gestión de parches quincenal -WSUS para los equipos Windows. Los Equipos Linux pueden ser gestionados directamente por TI. Entrenamiento al personal de TI sobre principios de seguridad básica y del porque es importante parchar los equipos al día y en donde pueden encontrar información sobre las vulnerabilidades de los sistemas basados CVEs
5	Hacker a través de malware, Ladrón a través de hurto del activo.	11,12	Creación de una política que cubra el manejo del material electrónico generado en la empresa. Entrenamiento del personal para que comprendan que es el ransomware y como no convertirse en una víctima.
6	Usuario interno no entrenado	12	Entrenamiento al personal para prevenir que divulguen información confidencial de la empresa en redes sociales. Clasificación de la información (sin restricción, clasificado, confidencial, Secreto corporativo).
7	Fallo infraestructura	3,9,10	Conectividad redundante con otro proveedor - Cable Modem corporativo como respaldo
8	Hacker	2,10,12	Sistema de detección de intrusos en cada estación. Instalación de un Cortafuegos corporativo que proteja al router principal Creación de las reglas adecuadas en el cortafuego.
9	Hacker mediante ataque remoto	3,9,10	Instalación y configuración de reglas en el cortafuego corporativo para botar los paquetes incompletos. Para esto se sugiera la implementación de un cortafuegos o firewall basado en IP tables (Linux)
10	Hacker	3,9,10	Política de cambio de claves cada 60 días.
11	Usuario interno	3, 9,10,12	Filtrado de IPs por direcciones MAC para disminuir la posibilidad de que se conecte un sistema no autorizado a la red interna.
12	Usuario interno	1,2,3,5,11,12	Implementación de las políticas de "último día en la oficina" - eliminar los accesos al mismo tiempo que se entrega una carta de despido, por ejemplo.
13	Hacker mediante Malware - Ransomware	11,12	Educación a los usuarios Política robusta de respaldos

14	Fallo de *hardware* en el equipo.	2,12	Reemplazo del sistema operativo en el servidor de archivos (Linux Mint 17.3) por uno especializado en la gestión de archivos (FreeNAS u OpenFiler)
15	Ladrón	12	Activación de las políticas de Google para empresas que permite administrar el dispositivo remotamente, permitiendo su borrado remoto.

Tabla 10 Listado de controles sugeridos para mitigar las amenazas sobre los activos identificados

Fuente: Elaboración propia.

4.2.4 Medir el impacto causado a la organización en caso de que el activo sufra de una materialización de una amenaza.

Una vez definidos cuáles son los controles que deben de aplicar, es necesario priorizarlos mediante la valoración económica del impacto, así como la posibilidad de ocurrencia.

Impacto	Calificación cualitativa	Calificación cuantitativa
Catastrófico	5	Pérdida superior a $ 10.000
Alto	4	Pérdida superior a $ 5.000
Medio	3	Pérdida superior a $ 2.500
Moderado	2	Pérdida superior a $ 1.000
Bajo	1	Pérdida superior a $ 500

Tabla 11 Escala de impacto en dólares.

Fuente: Elaboración propia basado en estimaciones de la edificadora.

Amenaza	Vulnerabilidad	Descripción del Impacto	Valoración Impacto

Hacker, otro colaborador de la empresa.	Usuarios no entrenados vulnerables a ingeniería social.	Acceso inapropiado a los sistemas y archivos de la empresa. Robo de Información.	5
Hacker a través de phishing	Usuario no entrenado en temas te seguridad de correo electrónico.	Robo/pérdida de Información	5
Hacker / atacante interno.	Políticas deficientes - Claves de usuario sin la adecuada protección - Ausencia de escritorio limpio	Robo de Información.	4
Hacker a través de malware / atacante externo.	Sistemas vulnerables.	Infección de equipos/Pérdida de información/Baja productividad por equipos degradados.	4
Hacker a través de malware, Ladrón a través de hurto del activo.	Gestión de respaldos no consistente, falta de políticas de seguridad con respecto al uso del material electrónico de la empresa.	Pérdida de información valiosa para la empresa por fallo, robo o infección	5
Usuario interno no entrenado	Usuario no entrenado para no compartir información en redes sociales	Un usuario no entrenado pudiera divulgar información importante que represente ventaja competitiva por compartir información en redes sociales de trabajo como Linkedin	4
Fallo infraestructura	Ausencia de conexión redundante	Como se determinó en el evalúo de los recursos requeridos para funcionar, un fallo en el internet deja a la empresa inactiva mientras el servicio se restaura, implicando impacto económico	4
Hacker	Puertos no utilizados abiertos y sin supervisión	Puertos abiertos no utilizados ni monitoreados representa una puerta de acceso para un atacante remoto en caso de que este localice un sistema vulnerable	5
Hacker mediante ataque remoto	Router no bota las conexiones abiertas incompletas	El router actual, al no estar debidamente configurado, es vulnerable a ataques sencillos de denegación de servicio.	4
Hacker	Claves del enrutador inalámbrico no se cambian de manera regular. Al tener la misma clave siempre, esta puede ser obtenida mediante ataques de fuerza bruta. Adicionalmente, al ser una clave vieja, existe la posibilidad que mucha gente la conozca	Denegación del servicio de red inalámbrico	2

Usuario interno	Falta de controles físicos para conectar equipo a los puntos de red en el edificio.	Un usuario podría conectar a la red un equipo que no sea propiedad de la empresa. Pudiendo cometer actos como hurto de información o incluso usar la conexión de internet para bajar material ilegal (películas, juegos, etc.), disminuyendo el ancho de banda disponible y exponiendo a la empresa a problemas legales.	4
Usuario interno	Falta de controles y procesos para la separación de empleados.	Un empleado descontento que sospecha que lo van a liquidar, podría robar información de la empresa o sabotear algún sistema	4
Hacker mediante Malware - Ransomware	Solución antivirus no detecta ataque de día cero, recayendo en los colaboradores de la empresa la responsabilidad de escoger que archivos abren de internet y cuáles no.	Un malware dentro de la red puede cifrar todos los documentos alojados en los equipos de la empresa, causando pérdidas importantes de información	5
Fallo de *hardware* en el equipo.	Servidor no configurado en espejo para proteger la información. Sistema de archivos con mediana tolerancia a corrupción de datos.	El servidor de archivos no cuenta con una configuración de espejo, por tanto, es vulnerable a un fallo físico de disco	5
Robo de teléfono celular con información de la edificadora en él	Robo de teléfono celular con información de la edificadora en él.	Información confidencial puede filtrarse, perdiendo ventaja competitiva.	5

Tabla 12 Valoración del impacto en términos monetarios. Escala de 1 a 5, 5 es el valor máximo.

Fuente: Elaboración propia basado en datos provistos por la edificadora.

4.2.5 Medir el riesgo residual luego de la aplicación de los controles

El nivel de riesgo no puede llevarse a cero sin desaparecer al activo, por eso se debe buscar un equilibrio entre el nivel de recursos y mecanismos que se ocupan para mitigar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente. La idea es que esta información sea compartida con la gerencia para que estos procedan a aceptar el

riesgo residual, transferirlo si es posible a través de un seguro o tomar medidas más extremas para disminuirlo aún más.

A continuación, se describe el riesgo residual que corresponde a como quedaron los riesgos luego de aplicar los controles.

ID Activo	Amenaza	Vulnerabilidad.	Probabilidad	Impacto después de controles	Riesgo Total
12	Hacker, otro colaborador de la empresa.	Usuarios no entrenados vulnerables a ingeniería social.	2	3	6
12	Hacker a través de phishing	Usuario no entrenado en temas te seguridad de correo electrónico.	5	2	10
	Hacker / atacante interno.	Políticas deficientes - Claves de usuario sin la adecuada protección - Ausencia de escritorio limpio	4	2	8
1,2,11 y 12	Hacker a través de malware / atacante externo.	Sistemas vulnerables.	4	2	8
11 y 12	Hacker a través de malware, Ladrón a través de hurto del activo.	Gestión de respaldos no consistente, falta de políticas de seguridad con respecto al uso del material electrónico de la empresa.	3	3	9
12	Usuario interno no entrenado	Usuario no entrenado para no compartir información en redes sociales	3	3	9
3,9 y 10	Fallo infraestructura	Ausencia de conexión redundante	2	3	6
2,10,12	Hacker mediante ataque remoto	Puertos no utilizados abiertos y sin supervisión	3	4	12
3,9,10	Hacker mediante ataque remoto	Router no bota las conexiones abiertas incompletas	3	3	9
3,9,10	Hacker	Claves del enrutador inalámbrico no se cambian de manera regular. Al tener la misma clave siempre, esta puede ser obtenida mediante ataques de fuerza bruta. Adicionalmente, al ser una clave vieja, existe	2	1	2

		la posibilidad que mucha gente la conozca			
3, 9,10,12	Usuario interno	Falta de controles físicos para conectar equipo a los puntos de red en el edificio.	3	3	9
1,2,3,5,11,12	Usuario interno	Falta de controles y procesos para la separación de empleados.	2	3	6
11,12	Hacker mediante Malware - Ransomware	Solución antivirus no detecta ataque de día cero, recayendo en los colaboradores de la empresa la responsabilidad de escoger que archivos abren de internet y cuáles no.	3	4	12
2,12	Fallo de *hardware* en el equipo.	Servidor no configurado en espejo para proteger la información. Sistema de archivos con mediana tolerancia a corrupción de datos.	2	4	8
12	Robo de teléfono celular con información de la edificadora en él	Robo de teléfono celular con información de la edificadora en él	2	4	8

Tabla 13 riesgo residual que corresponde a como quedaron los riesgos luego de aplicar los controles.

Fuente: Elaboración propia

Una vez obtenidos los resultados del análisis de riesgo, se procedió a compartir la información con la gerencia para que estos adquirieran mayor consciencia sobre su condición actual, pudieran decidir cuales controles están en capacidad de implementar y para los que no, planear y asignar presupuesto para los tiempos venideros.

Capítulo 5: Propuesta de solución

Una vez evaluado los riesgos, vulnerabilidades e impactos que pudieran afectar a los activos de Beta, en esta sección del documento se retoman los hallazgos para desarrollarlos más a fondo basado en las buenas prácticas de la industria de la seguridad de la información, así como en la experiencia personal del autor. Luego se preparará la documentación requerida para llevar a cabo dichas recomendaciones y servir de guía para su apropiada implementación.

5.1 Solución planteada con base en los hallazgos

A continuación de procedió a mapear los diferentes hallazgos, con las amenazas encontradas sobre los activos con el fin de plantear y ejecutar los controles para su debida mitigación.

5.1.1 Hallazgo 1: Colaboradores con poco conocimiento en temas de seguridad

5.1.1.1 Descripción

Luego de aplicar las encuestas, se determinó que los usuarios en general no tienen un conocimiento adecuado en temas de seguridad de claves y cuidados a la hora de bloquear los equipos cuando se alejan de estos y en general, ser más precavidos con las credenciales e información de la empresa que manejan.

5.1.1.2 Control a implementar

Se deben crear una serie de documentos para los entrenamientos en donde se les enseñe a los usuarios que es ingeniería social y como se puede causar daño a la empresa

usando las claves de otra persona para no ser detectados. Adicionalmente deben agregarse una serie de políticas que faciliten la adopción de buenas costumbres en el manejo de la información.

Parte del problema es que tanto la gerencia como los colaboradores en las empresas piensan más en ataques y hurtos de información de gente que no conocen y no se preocupan tanto de las personas que tienen a la par. Por ejemplo, en el caso de la edificadora, no se instruye a la gente que bloquee su terminal cuando se aleja de esta, lo que puede dejar al descubierto información sensitiva como un documento de planilla, fechas importantes para entrega de proyectos, dejar abierta una página web de un banco para el pago a proveedores, en fin, un sin número de información que puede ser expuesta en segundos.

5.1.1.3 Herramientas a utilizar

La herramienta a utilizar para solventar esta falencia es el criterio de COBIT 5, **DSS05.04** que consisten en gestionar la identidad del usuario y el acceso lógico, COBIT menciona que se debe:

> La identidad del usuario y el acceso lógico deben ser gestionados en base a las necesidades del negocio y del principio de menor privilegios. Una buena práctica es fortalecer los controles alrededor de la autenticación (es decir, el ID de usuario, la contraseña) y la autorización a los recursos sensibles. Uno debe asegurarse de que el acceso privilegiado o de administrador esté especialmente bien controlado y monitoreado (Greene, 2015, s. p.).

Se recomienda generar un procedimiento sobre gestión de cuentas y a la vez, generar el proceso de capacitación del mismo a los responsables del área en cuestión y mandos medios, de tal forma que sea posible extender la consciencia hacia los colaboradores sobre la importancia de cuidar sus credenciales y accesos.

5.1.2 Hallazgo 2: Colaboradores vulnerables a phishing

5.1.2.1 Descripción

En conversaciones con la gerencia, ellos comentaron sobre incidentes que han ocurrido en donde colaboradores de la empresa han caído en los correos de *phishing* buscando usuarios del Banco Nacional de Costa Rica y como sus cuentas se han visto comprometidas en varias ocasiones debido a este hecho.

5.1.2.2 Control a implementar

Se deben de crear una serie de documentos y entrenamientos en donde se les enseñe a los usuarios que sobre los diferentes tipos de ataques por medio de correo electrónico para lograr obtener información de cuentas bancarias, adicionalmente, como un control de refuerzo, se debe de montar un servidor de proxy que realice tareas de filtrado de sitios web, para ayudar a proteger a los usuarios de direcciones web con código malicioso. Para esta solución, se puede utilizar un servidor proxy de código abierto basado en SQUID.

5.1.2.3 Herramientas a utilizar

De nuevo, la educación del usuario se convierte en un factor indispensable para la protección de la información de la edificadora, por tanto, la implementación de políticas de protección de la información, así como la capacitación constante de los usuarios, es algo que no se puede dejar por fuera.

Aparte de la educación de usuarios, la otra herramienta a utilizar para en este caso sería tanto un control técnico como uno de procedimiento. COBIT 5, **DSS05.01** que consisten en Proteger contra *software* malicioso, COBIT menciona que se debe:

> Proteger contra *software* malicioso. Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del *software* malicioso (por ejemplo, virus, gusanos, –spyware- o spam (Greene, 2015).

Teniendo en cuenta que COBIT 5 recomienda la verificación de los filtros del tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, *software* espía y correos de *phishing*), esto se hace mediante la implementación de un control técnico de *software* y *hardware*. En este caso, se puede utilizar un servidor proxy de código abierto basado en SQUID.

SQUID tiene la ventaja de que por ser una herramienta de código abierto, no hay que incurrir en un gasto para su compra, adicionalmente el soporte de la herramienta es brindado por una gran comunidad de administradores que comparten su experiencia y brindan sus recomendaciones de administración y buenas prácticas sin ningún costo. Para el montaje de SQUID no se requiere de un servidor con muchos recursos. Asimismo es posible correr el *software* en forma de una máquina virtual, tanto para las pruebas como para su implementación final.

A la fecha de este escrito, el SQUID de pruebas se encuentra configurado en una máquina virtual, en donde se sigue probando su funcionamiento para que, una vez concluidas dichas pruebas, la solución puede ponerse en producción.

5.1.3 Hallazgo 3: Ausencia de escritorio limpio

5.1.3.1 Descripción

Se detectó la ausencia de escritorio limpio en algunas estaciones de trabajo de los colaboradores, en donde estos guardan claves debajo del teclado para evitar olvidos.

5.1.3.2 Control a implementar

Impulsar el uso de las áreas cerradas, protección de los dispositivos y sistemas de información, adoptar una cultura sin papel, así como inculcar el principio de escritorio limpio como parte de la cultura organizacional. Adicionalmente, se instaló en las estaciones de trabajo la solución de código abierto KeePass para la gestión de claves.

5.1.3.3 Herramientas a utilizar

La norma ISO 27001 recomienda contar con un escritorio limpio y su política respectiva, así como con todos los entrenamientos que esto conlleva.

La empresa debe considerar de forma periódica la educación las políticas y los procesos y de cómo estás faltas a las políticas puede conllevar a filtrados de información de la edificadora.

Entre algunos ejemplos de educación que seguirá utilizando la empresa se pueden citar el uso de carteles, alertas por correo electrónico, así como boletines con noticias. El encargado de TI será el responsable con la ayuda de la gerencia, de velar por dicha educación.

Adicionalmente, para facilitar la adopción de buenas prácticas de escritorio limpio para los colaboradores de la edificadora, se procedió a instalar el *software* de código abierto "**KeePass**", el cual permite guardar y gestionar las contraseñas del resto de los sistemas. Por tanto, los usuarios únicamente necesitan velar por una contraseña fuerte para esta aplicación y el resto de las claves pueden gestionarse desde allí. Para evitar la pérdida de

dichas claves, se gestionó una tarea de respaldo que copia el archivo cifrado con las claves en el servidor de archivos en un área de acceso restringido.

5.1.4 Hallazgo 4: Sistemas vulnerables a ciber ataques

5.1.4.1 Descripción

Mediante el escáner de vulnerabilidades, se detectaron una serie de sistemas que no están al día con los parches de seguridad.

5.1.4.2 Control a implementar

Instalación de un escáner de vulnerabilidades. Pueden utilizarse soluciones como las contenidas en la distribución de Linux para pruebas de penetración Kali Linux, así como Microsoft Baseline Security Analyzer de Microsoft.

Montaje de un sistema de gestión de parches quincenal -WSUS para los equipos Windows. Los Equipos Linux pueden ser gestionados directamente por TI.

Entrenamiento al personal de TI sobre principios de seguridad básica y del porque es importante parchar los equipos al día y en donde pueden encontrar información sobre las vulnerabilidades de los sistemas basados CVEs.

5.1.4.3 Herramientas a utilizar

La herramienta administrativa a utilizar para en este caso sería tanto un control técnico como uno de procedimiento. COBIT 5, **DSS05.01** que consisten en aplicar medidas preventivas para evitar el ataque a los sistemas, COBIT menciona que se debe:

> Proteger contra *software* malicioso. Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del *software* malicioso (por ejemplo, virus, gusanos, –spyware- o spam (Greene, 2015, s. p.).

Las herramientas técnicas utilizadas que se instalaron en la estación de trabajo del encargado de TI fueron las siguientes:

- "Microsoft Baseline Security Analyzer de Microsoft" para escanear los equipos corriendo el sistema operativo Windows. Este programa puede correrse de manera remota, lo que permite al encargado de TI conocer cuáles parches de seguridad están pendientes en los diferentes equipos y de donde puede descargar manualmente dichos parches de ser necesario.
- "Oracle VirtualBox" para correr máquinas virtuales en la máquina del encargado de TI.
- "Kali Linux" en forma de máquina virtual. Con esta herramienta es posible realizar escaneos de red, enumeración de dispositivos corriendo en la red, extracción de las direcciones MAC de los equipos, así como escaneos de vulnerabilidades, así como pruebas de penetración. Gracias al juego de herramientas contenidos en la distribución de Linux Kali, fue posible el detectar cuales equipos necesitaban cierto nivel de endurecimiento, dicho endurecimiento se realizó dependiendo del sistema operativo corriendo en cada equipo.

5.1.5 Hallazgo 5: Inconsistencias en las políticas de manipulación de la información.

5.1.5.1 Descripción

La mayoría de los colaboradores de la empresa generan contenido mediante la elaboración de estudios, diagramas y planos de los proyectos en los que trabajará la empresa. El problema radica en que no existe consistencia en donde se guardan los datos, mientras algunos trabajan y respaldan en el servidor de archivos, hay otros que trabajan con los archivos locales, por tanto, si el sistema falla, es robado y es infectado con *malware*, los datos corren el riesgo de perderse.

5.1.5.2 Control a implementar

Creación de una política que cubra el manejo del material electrónico generado en la empresa, así como entrenamiento del personal sobre la gestión de la información de datos digitales para que comprendan como debe de manipularse adecuadamente los datos.

5.1.5.3 Herramientas a utilizar

De nuevo COBIT 5 aparece como la herramienta administrativa a utilizar, ya que uno de sus procesos se denomina Gestión de la Continuidad (DSS04), perteneciente al dominio de entrega, servicio y soporte. Una de estas prácticas se relaciona con la Gestión de respaldo (DSS04.07), que tiene como fin mantener la disponibilidad de la información crítica para el negocio mediante la creación de un plan de copias de seguridad, así como el proceso de probar los resultados de las copias de seguridad de los datos para confirmar que estos han sido respaldados correctamente.

Las actividades que describe COBIT para este punto son:

- Respaldar los sistemas, aplicaciones, información y documentación de acuerdo a los horarios establecidos considerando:

- Frecuencia (mensual, semanal, diaria, etc.)
- Modo de respaldo (disco en espejo en tiempo real vs DVDs para retención a largo plazo)
- Tipo de respaldo (total vs incremental)
- Tipo de media.
- Respaldos automáticos en línea.
- Tipos de datos.
- Creación de bitácoras.
- Información crítica para el usuario (ejemplo, hojas electrónicas)
- Ubicación física y lógica de las fuentes.
- Seguridad y controles de acceso.
- Cifrado (Singh, 2015, s. p.).

Utilizando las buenas prácticas sugeridas por COBIT, se procedió a establecer un proceso de respaldos de información, así como una política más estricta para convencer a los usuarios de que deben de trabajar con los archivos desde el servidor de archivos y que, si desean mantener copias de los archivos en los equipos pueden hacerlo, pero que la prioridad es que estén en el servidor de archivos, el cual se encuentra configurado con un plan de respaldos regulares que incluye el respaldo de datos cifrados fuera del edificio. La edificadora ahora mantiene una copia de seguridad de sus datos cifrados en su bóveda de seguridad del Banco Nacional.

5.1.6 Hallazgo 6: Ausencia de políticas y entrenamientos que contemplen la información de la empresa que se puede compartir en redes sociales

5.1.6.1 Descripción

Se logró identificar 31 perfiles en la red social de profesionales Linkedin relacionados con la Edificadora Beta, sin embargo, no fue posible localizar una política u

entrenamiento en donde se eduque a los usuarios sobre qué clase de información de proyectos de Beta pueden compartir en esta red.

5.1.6.2 Control a implementar

Establecimiento de buenas prácticas y entrenamiento al personal para prevenir que divulguen información confidencial de la empresa en redes sociales, así como clasificación de la información (sin restricción, clasificado, confidencial, secreto corporativo).

5.1.6.3 Herramientas a utilizar

Como herramienta para cubrir este hallazgo, se tienen las buenas prácticas para la creación de una política de manejo de redes sociales.

David Gómez, presentador experto en temas comerciales y en redes sociales, escribió un artículo sumamente interesante y puntual en donde resalta cuales son los elementos que debe de incluir una política de manejo de redes sociales. De dicho artículo se pueden extraer las siguientes recomendaciones útiles:

> **Proteja la información sensible de la empresa:** Ser transparente con sus comunidades no significa que deba compartir la fórmula secreta. Hay cierto tipo de información que es de conocimiento exclusivo de la empresa y como tal debe respetarse (Gomez, 2013, s. p.).

Los colaboradores de la edificadora deben de ser entrenados en la nueva política se seguridad que solicita a los empleados en no divulgar información que podría comprometer la ventaja competitiva de la edificadora.

> **Verifique la cuenta desde la que publica:** Antes de dar clic al botón de publicar, siempre verifique que está compartiendo desde la cuenta correcta (Gomez, 2013, s. p.).

Cuando los colaboradores deseen participar en algún tipo de foro o comentar sobre algún tema de índole personal, tienen que verificar que lo estén haciendo desde una cuenta personal y no desde las cuentas de correo de la edificadora, ya que podría interpretarse que un comentario viene de la edificadora y no de la persona.

> **Plan de acción para manejo de crisis:** Tenga una instrucción clara de a quién llamar o con quién consultar, si estalla una crisis en las redes (especialmente en horas no laborables) (Gomez, 2013, s. p.).

Los colaboradores de Beta deben conocer los procesos que deben de seguir en caso de que se detecte una filtración de información, esto con el fin de remover dicha información de la manera más pronta y prevenir que este evento se repita.

> **Si tiene dudas, consulte:** Instruya al responsable de sus redes, que, si alguna persona hace un comentario, solicitud o pregunta específica y tiene dudas de la respuesta, se apoye en otras personas de la empresa que cuenten con la información correcta (Gomez, 2013, s. p.).

Si alguna persona externa trata de contactar a la edificadora a través de una red social y quién lo recibe no conoce el protocolo a seguir, el colaborador tiene que saber a quién contestar y el canal a usar para mantener siempre la imagen profesional de la empresa.

Con respecto a la mejora de proceso de clasificación de la información, este control debe de hacerse, sin embargo, queda en la lista de controles a implementar para después, pues dicha clasificación en un proyecto completo a mediano plazo, que amerita la participación de toda la empresa.

5.1.7 Hallazgo 7: Enlace de internet no redundante

5.1.7.1 Descripción

Observando el cuarto de telecomunicaciones y luego de confirmar las observaciones, se llegó a la conclusión de que a pesar de la alta dependencia que tienen las operaciones de día a día de la edificadora, ellos no cuentan con un enlace redundante que les permita seguir operando, aunque sea de forma degradada en caso de que el enlace principal caiga. Como la edificadora trabaja en el campo de licitaciones, la entrega tardía de una de estas licitaciones podría implicar la pérdida de un concurso y por ende un impacto importante al negocio.

5.1.7.2 Control a implementar

Conectividad redundante con otro proveedor – Cable Modem corporativo como respaldo

5.1.7.3 Herramientas a utilizar

En este momento, la edificadora se encontraba tramitando la instalación de un segundo enlace de internet para proveer el área de oficinas de dicho recurso, sin embargo, a la fecha, dicha instalación aún está pendiente.

5.1.8 Hallazgo 8: Puertos abiertos no utilizados

5.1.8.1 Descripción

Se detectaron puertos no utilizados abiertos y sin supervisión. En el caso de estaciones de trabajo de los colaboradores de la empresa, una máquina podría estar infectada y estar enviando virus tanto dentro como fuera de la red sin saberlo. En el caso de los servidores que tienen acceso directo a internet a través de una IP pública, el tener dichos puertos abiertos, facilita a un atacante externo un ataque directo al activo.

5.1.8.2 Control a implementar

Instalación de un cortafuegos corporativo que proteja al enrutador principal, así como la creación de las reglas adecuadas.

5.1.8.3 Herramientas a utilizar

Como solución de cortafuegos se instaló una máquina virtual en uno de los servidores con el fin de correr IPCop, que es una distribución de Linux especializada en realizar tareas de este tipo. La configuración del cortafuegos incluyó el cierre de todos los puertos no utilizados, lo que deja únicamente el puerto de VPN abierto para sustentar este servicio.

5.1.9 Hallazgo 9: Configuración incompleta en el enrutador

5.1.9.1 Descripción

Router no bota las conexiones abiertas incompletas, lo que da como resultado que este sea vulnerable a un ataque de denegación de servicio. Esto es, en caso de que un competidor de Beta quisiera que estos no participen en una licitación, podrían contratar a un atacante para que bote la conexión a internet mediante un ataque directo a esta vulnerabilidad.

5.1.9.2 Control a implementar

La función de cortafuegos se le delegó a la solución implementada en el control 8, por tanto, el IPCop ahora se encarga de esta función.

5.1.9.3 Herramientas a utilizar

La herramienta utilizada fue la distribución de Linux IPCop configurado como cortafuegos.

5.1.10 Hallazgo 10: Ausencia de política de ciclo de vida de claves.

5.1.10.1 Descripción

Las claves del enrutador inalámbrico no se cambian de manera regular, lo que facilita la entrada de un intruso a dicha red mediante el uso de herramientas de hackeo para redes inalámbricas.

5.1.10.2 Control a implementar

De acuerdo a la compañía de seguridad Acrylicwifi, creadores de soluciones de monitoreo de WiFi afirman que:

> Una contraseña WiFi de 12 caracteres es segura y no podrá ser descifrada con el poder de cómputo existente a día de hoy, ya que el tiempo necesario para crackear la contraseña crece de forma exponencial (Acrylicwifi, s. f., s. p.).

Tomando en consideración de que los puntos de acceso o Access Points ya estaban configurados con WPA2, lo único que hubo que hacer para mitigar esta amenaza fue incrementar la longitud de la clave a 12 caracteres, apagar el WPS (Wireless Protected Setup), que ya está ampliamente demostrado que es vulnerable, así como crear un procedimiento que regule el cambio de claves de los puntos de acceso cada 6 meses. El encargado de TI se comprometió a llevar a cabo este procedimiento.

5.1.10.3 Herramientas a utilizar

La herramienta que se utilizó para implementar este control consistió en buenas prácticas de la industria para la configuración de puntos de acceso inalámbricos.

La misma compañía Acrylic, publicó en su página web una serie de recomendaciones basadas en estudios elaborados por ellos mismos de acuerdo al poder computacional disponible en el año 2017.

A continuación, se transcriben las recomendaciones dadas por la compañía para asegurar una red WiFi y evitar que esta pueda ser hackeada por terceros:

> **PIN WPS (Wireless Protected Setup):** A nivel doméstico es habitual que los routers WiFi incluya soporte de la funcionalidad WPS para facilitar el intercambio de claves entre el punto de acceso y el usuario sin necesidad de usar la contraseña WiFi. Este proceso puede ser abusado con herramientas como Reaver o wpscrack y puede permitir obtener la clave de acceso a la red WiFi independientemente de su longitud o complejidad. La recomendación primera recomendación debe ser inhabilitar WPS si está soportado.
>
> **Nombre de la red WiFi:** El algoritmo de cifrado de WPA o WPA2 hace uso del nombre de la red WiFi para generar la clave criptográfica. Para evitar el uso de ataques de cracking con tablas rainbow se debe evitar usar un nombre de red conocido, como WLAN_66 y en su defecto usar nombres nuevos y que no identifiquen a la empresa o al usuario, como WLAN-YTQZFJ.
>
> **TKIP o AES CCMP:** Según el estándar 802.11, WPA usa un algoritmo llamado TKIP para firma y WPA2 usa el algoritmo AES CCMP que es mucho más robusto y elimina fallos de seguridad como “Beck-Tews attack” o “Ohigashi-Morii attack”. La recomendación es eliminar el soporte de TKIP si es posible, aunque a día de hoy los ataques no están lo suficientemente extendidos.
>
> **Redes publicadas:** La mayoría de dispositivos (teléfonos, ordenadores portátiles,) preguntan periódicamente a su alrededor la lista de redes conocidas solicitando esta información al aire, mediante el envío de un paquete WiFi conocido como frame de tipo Probe Request. Si un usuario configura incorrectamente la red WiFi y establece la contraseña como nombre de la red, cualquiera que se encuentre escuchando con un scanner WiFi como Acrylic podrá ver la contraseña de la red solicitada por el dispositivo del usuario.
>
> **Contraseñas de administración:** A nivel doméstico es habitual que el punto de acceso WiFi sea un router ADSL o un router de cable. Estos dispositivos pueden estar configurados con contraseñas de administración remotas como admin/admin, 1234/1234, support/support y accesibles desde Internet a través de HTTP con un navegador web. Se debe cambiar la contraseña de administración y limitar el acceso al panel de administración del router WiFi desde otras redes, como Internet, para evitar que un usuario pueda obtener la contraseña WiFi explotando un fallo de configuración del router WiFi desde internet (Acrylicwifi, s. f., s. p.).

5.1.11 Hallazgo 11: Falta de controles físicos para conectar equipo a los puntos de red en el edificio

5.1.11.1 Descripción

Falta de controles físicos para conectar equipo a los puntos de red en el edificio, con esto, es posible conectar dispositivos no homologados, que incluso podrían estar infectados por virus a la red interna, permitiendo actividades tales como descarga de contenido ilegal como películas y juegos e incluso, copias no autorizadas de los datos de la empresa.

5.1.11.2 Control a implementar

Filtrado de IPs por direcciones MAC para disminuir la posibilidad de que se conecte un sistema no autorizado a la red interna. Debido a que los Conmutadores de red (*switches*) de la empresa no cuentan con la capacidad de gestión remota, no es posible realizar el bloqueo por dirección MAC con los recursos actuales. Se recomienda el reemplazo de los 2 conmutadores por unos más modernos con la capacidad requerida de administración remota. Para mitigar este hallazgo mientras se cambian los equipos, se procedió a la creación de una política que limite la conexión de equipos únicamente por razones de trabajo y previa revisión del encargado de TI para prevenir infecciones y que no se permita dejar este tipo de equipos en la red por las noches.

5.1.11.3 Herramientas a utilizar

Política nueva que limite la conexión de equipos únicamente por razones de trabajo y previa revisión del encargado de TI para prevenir infecciones y que no se permita dejar este tipo de equipos en la red por las noches.

5.1.12 Hallazgo 12: La ausencia de controles y procesos para la separación de empleados

5.1.12.1 Descripción

Luego de la entrevista con la gerencia, se detectó la ausencia de controles y procesos formales para la separación de empleados, no existe un proceso en donde se describa el paso a paso de actividades que se deben de seguir cuando es necesario separar a un colaborador de la empresa, ya sea por retiro, renuncia o despido.

5.1.12.2 Control a implementar

Implementación de las políticas de "último día en la oficina" - eliminar los accesos al mismo tiempo que se entrega una carta de despido, por ejemplo.

5.1.12.3 Herramientas a utilizar

Cuando se separa a un colaborador, existe una serie de procesos que se deben seguir para cumplir con la ley, pero también hay que tomar en consideración medidas en lo que respecta a la seguridad de la información. Para esto, se puede utilizar como herramienta la norma **UNE-ISO/IEC 27002** que en su dominio de control Seguridad ligada a los recursos humanos, en la sección 8.3, señala que se deben de tomar una seria de medidas durante este proceso.

> Asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.
>
> Se deberían establecer responsabilidades para asegurar la gestión de la salida de los empleados, contratistas o usuarios de terceras partes de la organización y que se completa la devolución de todo el equipo y la cancelación de todos los derechos de acceso.

> Los cambios en las responsabilidades y las relaciones laborales dentro de la organización se deberían gestionar como la terminación de la respectiva responsabilidad o contrato laboral según esta sección y todas las contrataciones nuevas se deberían gestionar como se describe en el numeral 8.1 (International Organization for Standardization, 2013, s. p.)

En cuanto al personal saliente, el nuevo proceso de la edificadora contempla:

- Responsabilidades del ex empleado post contrato. Responsabilidades relacionadas tras la separación de la edificadora, con recordatorio de las relativas a la seguridad y las legales, como acuerdos de confidencialidad con respecto a los proyectos elaborados en la edificadora.

- Devolución de activos. La terminación del contrato laboral implicará la devolución de aquellos activos que el personal saliente pudiera tener en su posesión, bien *software* instalado, equipo de cómputo, documentos, planos, cotizaciones, información sobre licitaciones, etc.

- Revocación de los derechos de acceso. Deben de retirarse todos los accesos a los sistemas tras la terminación de contrato laboral al personal saliente.

5.1.13 Hallazgo 13: Equipos vulnerables a Malware – Falta de capacitación

5.1.13.1 Descripción

Solución antivirus no detecta ataque de día cero, los antivirus en general suelen ser vulnerables a esto, por lo que recae en los colaboradores de la empresa la responsabilidad de escoger que archivos abren de internet y cuáles no. Sin embargo los colaboradores no reciben una capacitación formal en este campo, por lo que ellos son el eslabón más débil en la cadena de seguridad de la información de la empresa.

5.1.13.2 Control a implementar

Para prevenir la pérdida de información en la edificadora y en las empresas en general, no solo es necesario contar con las herramientas y soluciones tecnológicas para este fin, deben estar acompañadas de dos componentes muy importantes, las políticas y la educación para fortalecer el eslabón más débil en materia de seguridad como lo es el usuario final. En otras palabras, para ayudar a disminuir el riesgo de ocurrencia de pérdida de información debido a *malware*, no solo se requiere el servidor de proxy montado como control del hallazgo 2, también es necesario que existan entrenamientos anuales sobre las amenazas digitales vigentes. Las notas que el responsable de TI envía para educar a los usuarios son sumamente útiles, pero también se necesita un programa de capacitación que sea semestral o anual, en donde se brinden y refresquen conocimientos sobre la seguridad de la información. Para este fin se recomienda contratar cada cierto tiempo a un profesional de seguridad para brinde charlas sobre las nuevas tendencias de los ataques y como no caer en ellos.

5.1.13.3 Herramientas a utilizar

La herramienta administrativa a utilizar para en este caso sería el criterio APO13.03 Supervisar y revisar el SGSI de COBIT 5, que establece:

> El sistema de administración de seguridad de la información general debe ser monitoreado y revisado regularmente (APO13.03) mediante revisiones de gestión y auditorías de seguridad. Un tema subyacente aquí es una cultura de seguridad y mejora continua (Greene, 2015, s. p.).

La gerencia se comprometió a asignar recursos para contratar a un profesional en seguridad a dar por lo menos una charla anual sobre temas de seguridad de la información y buenas prácticas.

5.1.14 Hallazgo 14: Servidor de archivos con oportunidades de mejora

5.1.14.1 Descripción

A nivel del servidor, se encontró un servidor de archivos de archivos basado en Linux, distribución Mint versión 17.3, la cual cuenta con actualizaciones de *software* garantizadas hasta abril del 2019. Dicho servidor cuenta con varios discos para el respaldo de datos. Sin embargo, no se encuentra configurado en espejo para proteger los datos en caso de un fallo de disco.

5.1.14.2 Control a implementar

Reemplazo del sistema operativo en el servidor de archivos (Linux Mint 17.3) por uno especializado en la gestión de archivos (FreeNAS u OpenFiler).

5.1.14.3 Herramientas a utilizar

Para solventar el problema encontrado, se procedió a la migración del servidor de archivos del sistema operativo actual, Linux Mint 17.3 a uno especializado en la gestión de archivos como lo es FreeNAS versión 9.10. La migración de los archivos se hizo mediante el uso de una unidad de almacenamiento externa, en donde se copiaron todos los datos, luego se procedió a la instalación del sistema operativo, la configuración de los discos existentes en espejo para otorgar tolerancia a fallos de *hardware*, la integración LDAP para permitir los accesos de usuarios manejados por el Active Directory para luego de esto, se procedió a la restauración de los archivos y las estructuras de estos para luego poner el sistema de nuevo en producción.

5.1.15 Hallazgo 15: Correo corporativo de la empresa en dispositivos de los empleados

5.1.15.1 Descripción

La gerencia manifestó su preocupación sobre el hecho de que sus colaboradores puedan tener el correo electrónico de la empresa configurado en el teléfono y de cómo ellos sienten que no tienen el control sobre los datos alojados ahí, ya que ellos utilizan la solución de Google para empresas. Sin embargo, luego de conversar con el encargado de TI, se llegó a la conclusión de que existen las herramientas para enviar políticas de seguridad desde la consola de administración de Google, no obstante, estas políticas no están implementadas.

5.1.15.2 Control a implementar

Activación de las políticas de Google para empresas que permite administrar el dispositivo remotamente, lo que permite la administración remota. En lo que respecta a las estaciones de trabajo, se recomienda el uso de cifrado de discos para proteger la información en caso de robo o pérdida del equipo.

5.1.15.3 Herramientas a utilizar

La herramienta administrativa a utilizar son las buenas prácticas dadas por el criterio DSS05.03 de COBIT 5 se describe a continuación:

> Se debe implementar y administrar la seguridad de punto final (*software* antivirus / antimalware, seguridad web / correo electrónico, cortafuegos) para asegurar que las computadoras portátiles, los equipos de sobremesa, los servidores y los dispositivos móviles estén adecuadamente protegidos (según el valor de la información). Los objetivos de alto valor (por ejemplo, joyas de la corona) deben ser protegidos con una seguridad y controles más fuertes (Greene, 2015, s. p.).

Para efectos técnicos, la herramienta a utilizar es la página de administración de "**Android for business**" de Google, en donde se detalla el paso a paso a seguir para configurar perfiles de trabajo que permite a una organización administrar todos los datos y aplicaciones corporativas importantes para la empresa, mientras el resto de datos del dispositivo permanecen bajo el control del usuario.

De acuerdo con Google, proveedor del servicio de correo de la edificadora, la configuración de perfiles de trabajo permite a los administradores realizar algunas o todas las acciones siguientes que se citan textualmente desde su página web de soporte.

> Mediante los perfiles de trabajo, los administradores pueden realizar algunas o todas las acciones siguientes:
>
> 1. Aplicar ajustes y restricciones por aplicación en los dispositivos.
> 2. Crear, eliminar y acceder a datos en el perfil de trabajo.
> 3. Instalar y quitar aplicaciones y certificados de forma silenciosa
> 4. Solicitar una lista de las aplicaciones que acceden a los datos del dominio de trabajo en el perfil de trabajo
> 5. Borrar datos del perfil de trabajo de forma remota
> 6. Restringir el contenido que se puede compartir entre el perfil personal y el de trabajo.
> 7. Bloquear la capacidad de realizar capturas de pantalla en el perfil de trabajo.
> 8. Ver estadísticas relacionadas con tu cuenta administrada
> 9. Administrar el acceso corporativo al servidor de correo y a los datos internos
> 10. Cambiar la contraseña de la cuenta
> 11. Supervisar la actividad de red y la información de ubicación (Google, s. f., s. p.).

Según las instrucciones brindadas en la página de soporte de Google, fue posible establecer las políticas de seguridad para el control de los dispositivos móviles que pertenecen a la empresa. Adicionalmente fue necesario generar una política y un

documento de instrucciones en donde se le explica al colaborador que desee instalar el correo de la empresa en el teléfono sobre las condiciones que debe de aceptar para poder hacer uso de este servicio.

Para efectos de las estaciones de trabajo, la solución propuesta consiste en la activación del servicio de cifrado completo de disco que viene integrado con Windows, conocido como Bitlocker.

5.2 Hallazgos clasificados por dominio

Luego de identificar cada una de las falencias de seguridad, se procedió a clasificarlas en dominios de acuerdo a la naturaleza de cada hallazgo y presentar la información en tablas para facilitar el proceso de medición del progreso por dominio.

5.2.1 Hallazgos – Ausencia de conciencia de seguridad de la Información

Hallazgo	Control Propuesto	¿Se Implementó?
Gestión de claves: Poco cuidado a la hora de bloquear los equipos	Procedimientos sobre gestión de cuentas + capacitación + soporte gerencial + monitoreo.	SI
Phishing: Correos de *phishing* buscando usuarios del BNCR en donde los usuarios han sido engañados.	Documentos y entrenamientos.	En Progreso
	Servidor proxy basado en SQUID	
Escritorio limpio: Información sensitiva sin protección.	Capacitación de los usuarios en este tema.	SI
	Herramienta de gestión de claves – KeePass	
Capacitación: Equipos vulnerables a Malware – Falta de capacitación.	Proxy (SQUID) del hallazgo 2.	SI
	Educación constante a los usuarios.	
	Campañas de concientización.	

Capacitación: Uso de redes sociales (31 perfiles identificados)	Políticas + Entrenamiento al personal en el uso de redes sociales.	En Progreso

Tabla 14 Hallazgos – Ausencia de conciencia de seguridad de la Información.

Fuente: Elaboración propia

5.2.2 Hallazgos – Gobernanza de TI

Hallazgo	**Control Propuesto**	**¿Se Implementó?**
Políticas: Inconsistencias en el manejo de la información. No siempre se guardan los datos en el servidor de archivos.	Creación de políticas que cubran el manejo del material electrónico generado en la empresa.	SI
	Capacitación + apoyo de la gerencia a las nuevas políticas.	
Políticas: Ciclo de vida de claves en los enrutadores inalámbricos.	Buenas prácticas de la industria para la configuración de puntos de acceso inalámbricos.	SI
Políticas y procedimientos: La ausencia de procedimiento y procesos para la separación de empleados	Creación de procedimientos de separación (UNE-ISO/IEC 27002).	En progreso
Políticas y Procedimientos: Correo corporativo de la empresa en dispositivos de los empleados.	Activación de las políticas de Google para empresas que permite administrar el dispositivo remotamente, permitiendo administración remota	SI

Tabla 15 Hallazgos – Gobernanza de TI.

Fuente: Elaboración propia

5.2.3 Hallazgos – Arquitectura y Diseño de Seguridad de la red

Hallazgo	Control Propuesto	¿Se Implementó?
Diseño: Puertos abiertos no utilizados en servidores. Se detectaron puertos no utilizados abiertos y sin supervisión.	"cortafuegos" - Herramienta de código abierto IPCOP.	SI
	Inhabilitación de servicios no utilizados.	
Arquitectura: El enrutador no cuenta con la capacidad requerida. Router no bota las conexiones abiertas incompletas (**DDOS**).	Regla en "cortafuegos" – IPCOP.	SI
Diseño: Servidor de archivos con oportunidades de mejora.	Reemplazo del sistema operativo en el servidor de archivos por uno especializado en la gestión de archivos (FreeNAS)	SI
Diseño: Se detectaron una serie de sistemas que no están al día con los parches de seguridad.	WSUS para administrar y distribuir actualizaciones en los equipos Windows. Entrenamiento a los colaboradores del área de TI.	En Progreso
Diseño: Es posible conectar equipos no autorizados a los puntos de red localizados en cada una de las oficinas.	Filtrado de IPs por direcciones MAC.	En Progreso
	Inventario de dispositivos.	

Tabla 16 Hallazgos – Arquitectura y Diseño de Seguridad de la red.

Fuente: Elaboración propia

5.2.4 Hallazgos – Planes de continuidad del negocio Recuperación de Desastres.

Hallazgo	Control Propuesto	¿Se Implementó?
Enlace de internet no redundante.	Conectividad redundante con otro proveedor – Cable Modem corporativo como respaldo	NO

Tabla 17 Hallazgos – Planes de continuidad del negocio Recuperación de Desastres.

Fuente: Elaboración propia.

Capítulo 6: Conclusiones y recomendaciones

6.1 Conclusiones

Durante el desarrollo de la parte de investigación del proyecto, se evidenció la situación actual que viven las pequeñas empresas en nuestro país. Muchas de estas no conocen de la existencia de buenas prácticas en el campo de la seguridad de la información y por tanto no son conscientes de los problemas que conlleva no gestionar la seguridad de la información y el tratamiento de los riesgos. Un ejemplo claro fue la Edificadora Beta, ellos tenían presente la existencia de algunos de los hallazgos resultantes del análisis, sin embargo, no sabían cómo gestionarlos.

En Costa Rica gobierno de la seguridad de la Información y las buenas prácticas de la industria no se han sido difundido de una manera efectiva, por lo que son muy pocos los profesionales que están preparados para guiar a las organizaciones hacia un modelo sostenible de seguridad de la información. A esto se le debe de sumar el hecho de que la seguridad de la información no trae una entrada económica cuando se aplica, sino que más bien protege de una posible pérdida al materializarse las brechas de seguridad. Este es un factor importante a la hora de convencer a la alta gerencia sobre su importancia y necesidad.

Luego de que la edificadora aceptara que se hiciera el estudio y que brindara la información pertinente, se procedió al estudio de las políticas y de los procedimientos existentes, para investigar si contemplaban como proteger la información de la empresa mediante la comparación de estas contra las buenas prácticas de la industria mediante

marcos como COBIT e ISO y así poder dictar un resultado del estado en este campo de la empresa. Para realizar esta tarea, fue necesario profundizar en los diferentes marcos de buenas prácticas, estudiarlos y ver qué criterios serían los indicados para poder evaluar la situación de la edificadora.

Los resultados obtenidos no fueron malos, ya que la gerencia, a pesar de no conocer de la existencia de las buenas prácticas de la industria o de marcos para las buenas prácticas, si se esmeraban en hacer las cosas bien. Esto lo demuestra la presencia de políticas generales sobre la confidencialidad de la información, sin embargo, no estaba contemplada la seguridad de la información como parte de la cultura organizacional de la edificadora.

El objetivo final se logró mediante el desarrollo de la propuesta del plan de seguridad para la constructora que consta de modificaciones a las política y procedimientos de la empresa, así como el plan de ejecución que conllevó a la participación del personal de diferentes departamentos durante la exploración, la implementación y mejora de procesos aplicando medidas preventivas y correctivas para reducir los niveles de riesgo existentes, además de reconocer el nivel de riesgo residual luego de los controles implementados a los cuales aún se encuentran expuestos los sistemas de la organización.

Algunos de los controles sugeridos tienen un costo, por lo que en cada caso en particular se sigue el principio de evaluar el valor de la información a proteger vs los costos que implicarían la pérdida y/o impacto de un ataque y basado en ese principio, planificar las acciones correspondientes para la protección de dicho activo.

6.2 Recomendaciones

Como recomendación final, hay que enfatizar el hecho de que la gestión de riesgos en una empresa debe considerarse un proceso necesario y constante, ya que si la organización no conoce sobre el riesgo que corren sus activos, difícilmente llegará a estar preparada para evitar o mitigar una posible brecha. De allí la importancia de tener dicho proceso para gestionar sus riesgos y así crear y actualizar controles para disminuir la posibilidad de que estos se materialicen.

En general, en nuestro país el departamento de TI es comúnmente el encargado de determinar los proyectos y contrataciones a efectuar, cuenta en su mayoría con presupuestos pequeños debido a que la gerencia considera que TI no requiere de asignación de muchos recursos para realizar su trabajo. Por tanto, solicitar recursos para proyectos de seguridad suele ser algo impensable en las empresas hoy en día. Una recomendación muy importante consiste en educar a la gerencia sobre las necesidades reales de la seguridad de la información y de cómo su ausencia puede impactar negativamente la expectativa de vida de la empresa, como los ejemplos que se mencionaron durante el desarrollo de este proyecto.

Bibliografía

Acrylicwifi (s. f.). *¿Es segura una red WiFi con WPA y WPA2?* Obtenido de acrylicwifi.com: https://www.acrylicwifi.com/blog/es-segura-red-wifi-wpa-wpa2/

Avedaño, M. (31 de Agosto de 2015). *CCSS denuncia 'hackeo' de 500.000 registros del sistema de planillas*. Obtenido de La Nacion.com: http://www.nacion.com/sucesos/crimenes-asaltos/CCSS-denuncia-funcionarios-financiera-registros_0_1509249216.html

Canonical (2017). *ZFS*. Obtenido de Ubuntu Wiki: https://wiki.ubuntu.com/ZFS

Catoira, F. (28 de Enero de 2013). *Uso de filtros en Wireshark para detectar actividad maliciosa*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2013/01/28/uso-filtros-wireshark-para-detectar-actividad-maliciosa/

CERT - Carnegie Mellon University ((s. f.). *OCTAVE.* Obtenido de Carnegie Mellon University Web Site: http://www.cert.org/resilience/products-services/octave/index.cfm

CGR (21 de Junio de 2007). *Normas técnicas para la gestión y control de TI.* Obtenido de http://ocu.ucr.ac.cr: http://ocu.ucr.ac.cr/images/ArchivosOCU/CapacitacionRIDS/N-2-2007-CO-DFOENormasGestionControlTI-CGR.pdf

Chacón, K. (20 de Setiembre de 2015). *Hackeo en CCSS enciende alarmas en seguridad de datos personales*. Obtenido de elfinancierocr.com:

http://www.elfinancierocr.com/tecnologia/CCSS-hackeo-extraccion_de_datos-BAC_San_Jose-seguridad_informatica_0_813518666.html

Comunidad SQUID. (2013). *Squid: Optimising Web Delivery*. Obtenido de squid-cache.org: http://www.squid-cache.org/

Consejo Superior de Administración Electrónica de España (2012). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Obtenido de PAE - Portal de Administración Electrónica.: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WWucMojyuUk

Consejo Superior de Administración Electrónica de España (2012). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Obtenido de administracionelectronica.gob.es: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WWucMojyuUk

Ezquieta, J. (16 de Junio de 2013). *Manual del Administrador de IPCop v2.0.0*. Obtenido de ipcop.org: http://www.ipcop.org/2.0.0/es/admin/html/

FreeNAS (2017). *What is FreeNAS?* Obtenido de freenas.org: http://www.freenas.org/

Gomez, D. (3 de octubre de 2013). *Cómo diseñar una política de manejo de redes sociales*. Obtenido de http://bienpensado.com: http://bienpensado.com/politica-redes-sociales/

Google (s. f.). *¿Qué es un perfil de trabajo?* Obtenido de Google: https://support.google.com/work/android/answer/6191949

Greene, F. (2015). *Selected COBIT 5 Processes for Essential Enterprise Security*. Obtenido de isaca.org: https://www.isaca.org/Journal/archives/2015/Volume-2/Pages/selected-cobit-5-processes-for-essential-enterprise-security.aspx

International Organization for Standardization (2013). *Information technology -- Security techniques -- Code of practice for information security controls*. Obtenido de ISO.ORG: https://www.iso.org/standard/54533.html

ircrack-ng ((s. f.). *Aircrack-ng*. Obtenido de Aircrack-ng - Descripction: https://www.aircrack-ng.org/

ISACA (2012). *COBIT 5 Spanish.* Obtenido de ISACA.ORG: http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

ISACA ((s. f.). *Glossary.* Obtenido de https://www.isaca.org/Pages/Glossary.aspx?

ISACA ((s. f.). *ISACA Glossary of Terms.* Recuperado el 15 de Julio de 2017, de isaca.org: https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

ISO27000.ES ((s. f.). *ISO 27000.* Recuperado el 16 de Julio de 2017, de iso27000.es: http://www.iso27000.es/download/doc_iso27000_all.pdf

La Vanguardia (15 de 12 de 2016). *La web de citas para infieles Ashley Madison paga para cerrar la investigación por el pirateo*. Obtenido de lavanguardia.com: http://www.lavanguardia.com/economia/20161215/412638797817/ashley-madison-multa-citas-infiel-pareja.html

MICITT (26 de Agosto de 2015). *Costa Rica avanza en uso y legitimidad de Firma Digital*. Obtenido de http://micit.go.cr: http://micit.go.cr/index.php?option=com_content&view=article&id=6745:costa-rica-avanza-en-uso-y-legitimidad-de-firma-digital&catid=40&Itemid=630

Microsoft Corp (2017). *Microsoft Baseline Security Analyzer*. Obtenido de https://technet.microsoft.com/es-es/security/cc184924.aspx

Microsoft ((s. f.). *Introducción al Cifrado de unidad BitLocker*. Obtenido de microsoft.com: https://technet.microsoft.com/es-es/library/cc732774(v=ws.11).aspx

nmap.org ((s. f.). *Guía de referencia de Nmap (Página de manual)*. Obtenido de https://nmap.org/man/es/index.html

nmap.org ((s. f.). *Zmap*. Obtenido de nmap.org: https://nmap.org/zenmap/

Offensive Security ((s. f.). *What is Kali Linux?* Recuperado el Julio de 2017, de docs.kali.org: https://docs.kali.org/introduction/what-is-kali-linux

Oracle ((s. f.). *Welcome to VirtualBox.org!* Obtenido de virtualbox.org: https://www.virtualbox.org/

Reichl, D. (s. f.). *What is KeePass?* (D. Reichl, Editor) Recuperado el 07 de Junio de 2017, de keepass.info: http://keepass.info/

Reuters (25 de Agosto de 2014). *Hackean servicio de PlayStation Network de Sony*. Obtenido de forbes.com.mx: https://www.forbes.com.mx/hackean-servicio-de-playstation-network-de-sony/

Rhodes, T., Jude, A., Reuschling, B., & Block, W (2017). *Chapter 19. The Z File System (ZFS)*. Obtenido de freebsd.org: https://www.freebsd.org/doc/handbook/zfs.html

Rodríguez, G. (22 de 08 de 2015). *Todo lo que necesitas saber sobre el 'caso Ashley Madison'*. Obtenido de huffingtonpost.es: http://www.huffingtonpost.es/2015/08/22/ashley-madison_0_n_8020140.html

Schneier, B. (15 de Septiembre de 1999). *Crypto-Gram*. Obtenido de https://www.schneier.com: https://www.schneier.com/crypto-gram/archives/1999/0915.html#OpenSourceandSecurity

Singh, A. (12 de Mayo de 2015). *COBIT 5: Managing Continuity Aspects with a practical approach.* Obtenido de isaca.org: http://www.isaca.org/chapters4/Adelaide/Events/Documents/BCM_CoBIT%205_ISACA_ASingh.pdf

Symantec (s. f.). *Glosario*. Recuperado el 31 de Julio de 2017, de symantec.com: https://www.symantec.com/es/mx/security_response/glossary/define.jsp?letter=v&word=virtual-machine

Symantec (s. f.). *Glosario*. Recuperado el 31 de Julio de 2017, de symantec.com: https://www.symantec.com/es/mx/security_response/glossary/define.jsp?letter=m&word=mac-address

Thomas, K. (31 de 08 de 2015). *Caso Ashley Madison: la cronología de los hechos*. Obtenido de welivesecurity.com: http://www.welivesecurity.com/la-es/2015/08/31/caso-ashley-madison-cronologia/

Anexos

Anexo 1: COBIT.

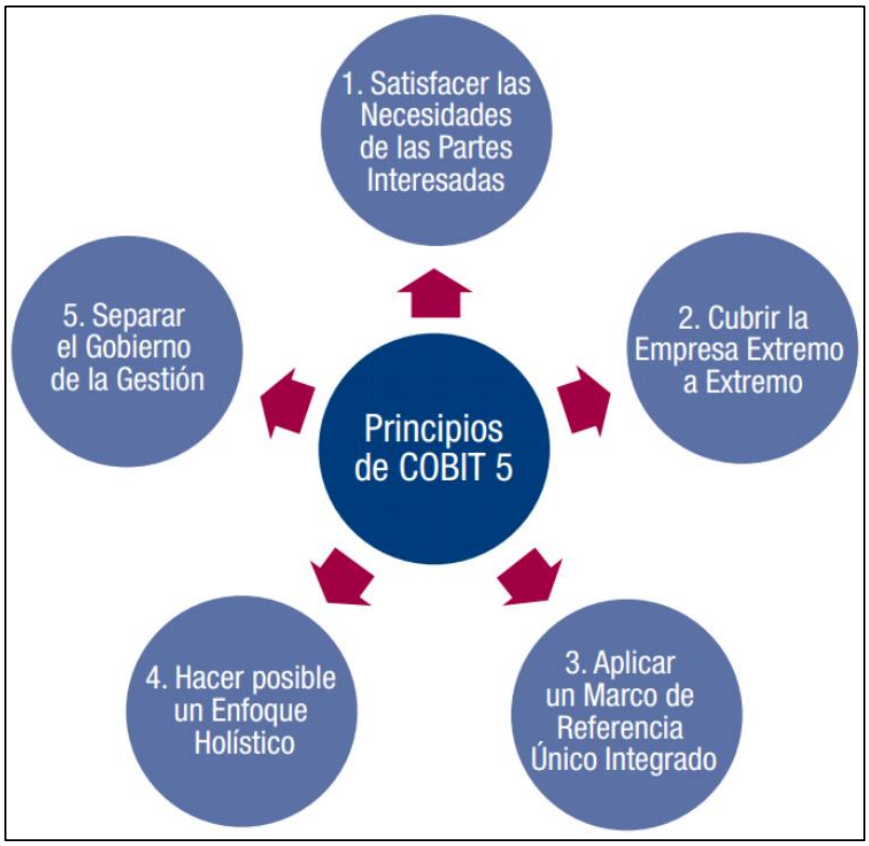


Figura 15 Principios de COBIT.

Fuente: IT Governance Institute, COBIT 2012

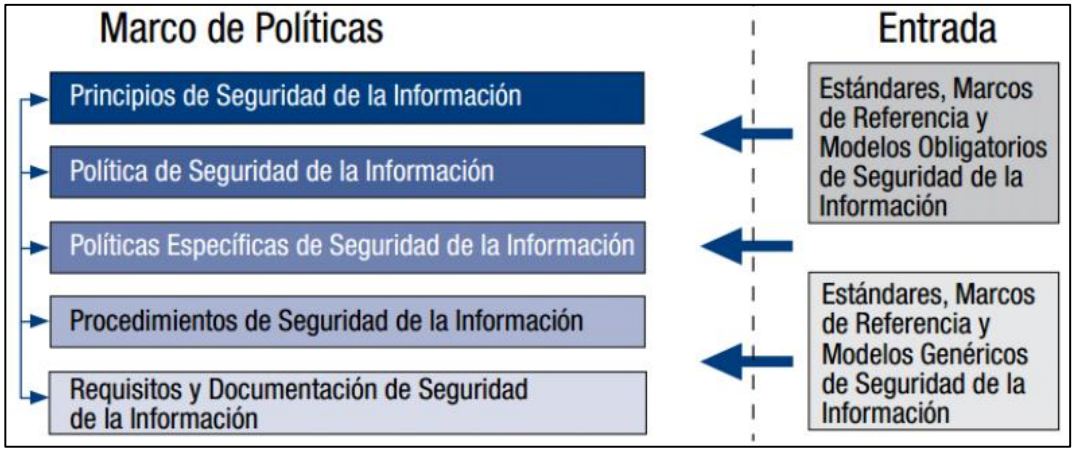


Figura 16 Marco de políticas.

Fuente: IT Governance Institute, COBIT 2012

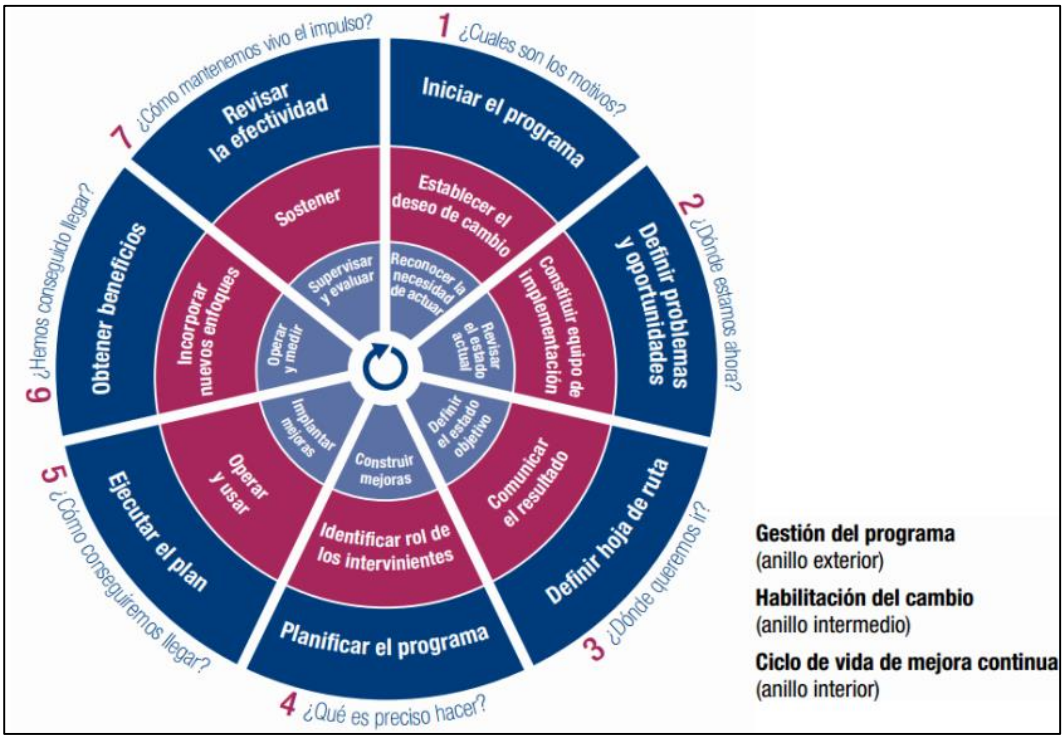


Figura 17 Fases de implementación de COBIT.

Fuente: IT Governance Institute, COBIT 2012

Anexo 2: Lista de verificación de la seguridad física – Cuestionario.

Fuente: Curso MSEG-04 - Control de acceso, seguridad ambiental y física (impartido por el profesor Claudio Valverde)

5.2.5 Barreras Del Perímetro - Instalaciones

1. ¿Un cercado u otra barrera física define el perímetro de la instalación?

a. Especificar el tipo y la altura de la barrera física. *Concreto en la base, malla en el medio y alambre navaja en la parte de arriba.*
b. Describir la condición de las barreras físicas. *Buenas condiciones. Buena visibilidad e iluminación.*
c. ¿Se considera que la barrera perimetral es una garantía de seguridad? *Se considera parte de una solución integral.*
d. ¿La barrera perimetral está a 7 metros o más de los límites de la propiedad de la instalación? *Sí, sin embargo, en ocasiones este espacio se utiliza para parquear vehículos cuando está muy lleno.*
e. ¿La barrera perimetral está bajo vigilancia en todo momento? *Sí, tiene cámaras monitoreadas en todas esquinas y cuenta con buena iluminación.*

2. Si se utiliza una valla de eslabones como barrera perimetral,

a. ¿Está construida de un alambre calibre #11 o superior? *No podría asegurar el calibre del alambre, pero si se ve bastante robusto.*
b. ¿La abertura de la malla no tiene más de dos pulgadas cuadradas? *No, la abertura es adecuada. No se puede meter la mano.*
c. ¿Los extremos están reforzados y con púas o alambre navaja en la parte
d. superior? *Sí, alambre navaja.*
e. ¿Está la parte inferior de la valla reforzada y extendida dentro del suelo? *Sí, con concreto.*

3. Si el edificio forma parte de la barrera perimetral, --No aplica.

a. ¿Presenta un peligro en el punto de unión con el cercado perimetral? *NA*
b. ¿Tiene puertas, ventanas u otras aberturas del lado del perímetro? *NA*

4. Si un río o lago forma alguna parte del límite del perímetro, ¿se proporcionan medidas adicionales de seguridad? –No aplica.

5. ¿Hay aberturas tales como alcantarillas, túneles, pozos de acceso para alcantarillas y acceso a servicios públicos, que permitan el acceso a la instalación?

No. El perímetro está bien cerrado.

6. Describa las características físicas de cada entrada del perímetro.

Existen 2 entradas al perímetro, en donde solo una de ellas se utiliza regularmente, la otra se cómo la puerta trasera, pero se encuentra cerrada con cierre eléctrico y tiene una cámara vigilándola todo el tiempo, tiene buena iluminación de noche (el monitor está en la recepción, en donde la recepcionista puede ver lo que pasa). La entrada principal está igualmente monitoreada con cámaras, buena iluminación, cierre eléctrico y timbre.

7. ¿Están protegidos o asegurados todos los puntos de entrada en las barreras perimetrales?

Sí, no es posible entrar sin llevar una escalera muy alta o sin violentar el cerrojo principal, que de hecho es bastante robusto.

8. ¿Están construidas todas las entradas perimetrales de materiales adecuados y han sido instaladas de tal forma que proporcionan protección equivalente a las barreras perimetrales de las que forman parte?

Sí, debido a que la actividad de la empresa es de construcción de obras, es de esperar que los materiales sean de primera y todo bien diseñado.

9. ¿Las entradas perimetrales que no están en uso frecuentemente son inspeccionadas por guardias u otro personal?

No, debido a que tienen cámaras 24x7, con buena iluminación. También cuenta con alarma durante la noche en caso de que fuercen la entrada cuando solo está el guarda.

10. ¿El responsable de seguridad es responsable de la seguridad de las llaves en las entradas perimetrales?

Sí, el guarda tiene acceso a todo el edificio. Según la gerencia, es alguien de mucha confianza. El guarda está en la planilla de la empresa y ha estado en su puesto por más de 10 años.

11. ¿Las llaves de las entradas perimetrales se brindan a otro personal que no es el de la instalación, como el personal de contratistas?

No, si alguien visita la instalación, tiene que estar escoltado, debido a que para reunirse con alguien allí, hay que sacar cita, no entra público en general.

12. ¿Están iluminadas todas las entradas de peatones y de vehículos normalmente utilizadas y otras entradas de perímetro? para asegurar:

a) Identificación adecuada de las personas y verificación de las credenciales. *SI*

b) Que los interiores de los vehículos están claramente iluminados; *SI*

c) El resplandor de las luminarias no afecta los ojos de los guardias. *SI*

13. ¿Hay letreros adecuados en los que se establecen las disposiciones de entrada claramente colocadas en todas las entradas principales?

Sí, el letrero está bien ubicado, es grande y visible

14. ¿Hay letreros de "No entre" colocados o adyacentes a las barreras perimetrales a intervalos tales que al menos un signo es visible en cualquier aproximación a la barrera en una distancia mínima de 45 metros?

No, no se divisó ningún letrero de "No entre", solamente el clásico, "no estacione" en la entrada.

15. ¿Se mantienen zonas claras en ambos lados de la barrera perimetral?

Sí, en la mayoría de los casos, el área se encuentra despejada.

16. ¿Se permite el estacionamiento de automóviles contra o cerca de barreras perimetrales?

Sí, por razones de espacio, se permite el estacionar vehículos tanto afuera de la valla como adentro.

17. ¿Se permite que madera, cajas u otros materiales se apilen contra las barreras perimetrales o cerca de ellas?

No, en general, no llega mucho material a las instalaciones, adicionalmente se denota orden dentro del espacio físico.

18. ¿Los guardias patrullan las áreas perimetrales?

No, solo de noche. Sin embargo, el espacio perimetral externo no es muy grande como para que alguien se oculte de las cámaras.

19. ¿Los guardias observan y reportan factores inseguros relacionados con las barreras perimetrales?

Sí, de acuerdo con los colaboradores de la empresa, cuando algo raro se ve en la valla, se reporta inmediatamente.

20. ¿Está provisto un camino interior de perímetro para el uso de vehículos de patrulla de guardia? Si es así, ¿cuál es la condición?
No, no aplica.

21. ¿Los perímetros están protegidos por dispositivos de alarma de intrusión?

Sí, se confirmó la presencia de sensores de movimiento en la zona perimetral.

5.2.6 Iluminación Para Protección

22. ¿El perímetro de la instalación está protegido por la iluminación?

Sí, el perímetro de la instalación cuenta con muy buena iluminación, que permanece encendida toda la noche.

23. ¿La iluminación de protección proporciona un medio para continuar durante las horas de oscuridad el mismo grado de protección disponible durante las horas de luz del día?

Sí, el perímetro de la instalación cuenta con muy buena iluminación.

24. ¿Están los conos de iluminación de las lámparas dirigidas hacia abajo y lejos de las instalaciones propias y lejos del personal de guardia?

Sí, La mayoría de las luces cumplen con este requisito. Existen algunas que se encuentran cerca de la valla.

25. ¿Están instaladas las luces para proporcionar una cadena de luz dentro y fuera del cercado?

Sí, la iluminación en la valla es adecuada.

26. ¿Se comprueba si las luces funcionan correctamente antes de la oscuridad?

No, Las bombillas se cambian reactivamente.

27. ¿Las reparaciones a las luces y el reemplazo de lámparas no operativas se realizan inmediatamente?

Sí, hay algunas bombillas de repuesto dentro del edificio

28. ¿Los rayos de luz se superponen para proporcionar cobertura en caso de que una bombilla se queme?

Sí, No se encuentran muy distanciadas, a simple vista podría decirse que es suficiente para notar la presencia de un intruso, pero no para identificarlo.

29. ¿Se proporciona iluminación adicional en las entradas activas y puntos de posible intrusión?

Sí, las entradas cuentan con sus propias bombillas.

30. ¿Las cabinas de los guardias de las entradas están provistas de la iluminación adecuada?

No, No existe una cabina externa, el guarda permanece en la recepción vigilando las cámaras y haciendo rondas.

31. ¿Se utilizan acabados ligeros o rayas en las partes inferiores de edificios y estructuras para ayudar a la observación de guardias?

No, la decoración del edificio es tradicional, no está pensado en facilitar la visibilidad de los guardas.

32. ¿Tiene la instalación una fuente confiable de energía para su sistema de iluminación?

No, si falla la energía eléctrica, solo la alarma tiene soporte por baterías.

33. ¿Tiene la instalación una fuente auxiliar de energía confiable?

No, si el fluido eléctrico falla, no hay energía de reserva.

34. ¿Es el sistema de iluminación de protección independiente de la iluminación de la instalación general o sistema de energía?

El sistema de iluminación se encuentra conectado a la instalación general.

35. ¿Se protege adecuadamente la fuente de alimentación de las luces?

Las luces están a buena altura, sin embargo, sí podrían ser destruidas con piedras o palos.

36. ¿Hay provisión para iluminación de emergencia?

No, solo las baterías internas del equipo.

37. ¿Se prueba el equipo de emergencia con frecuencia?

Sí, Solo las alarmas y las luces de emergencia funcionan. Las luces de emergencias son más pensadas para la gente que no se tropiece si falla la luz dentro del edificio, no para la seguridad del mismo.

38. ¿Se ha diseñado el equipo de emergencia para que entre en funcionamiento automáticamente cuando sea necesario?

Las luces de emergencias son más pensadas para la gente que no se tropiece si falla la luz dentro del edificio, no para la seguridad del mismo.

39. ¿Está correctamente instalado el cableado para la iluminación de protección?

a) ¿Está en conductos resistentes a la manipulación? *NO*
b) ¿Está instalado bajo tierra? *NO*
c) Si está sobre el suelo, ¿es lo suficientemente alto como para reducir la posibilidad de manipulación? *SI*

40. ¿Se encuentran, controlan y protegen adecuadamente los interruptores y controles?

a) ¿Son resistentes a la intemperie y a la manipulación? *SI*
b) ¿Son fácilmente accesibles para el personal de seguridad? *SI*
c) ¿Están localizados de manera que sean inaccesibles desde fuera de la barrera perimetral? *SI*
d) ¿Existe un interruptor situado de forma centralizada para controlar la iluminación de protección? *NO*

41. ¿Hay una iluminación adecuada para el uso de guardias en las rutas interiores?

Sí, El perímetro completo está bien iluminado.

42. ¿Están los materiales y equipos en las áreas de envío y almacenamiento adecuadamente dispuestos para no enmascarar la iluminación de seguridad?

5.2.7 Alarmas De Protección

43. Si se utiliza un sistema de alarma en la instalación, ¿qué dispositivo de detección se utiliza?

a) ¿Es un sistema de alarma local? *SI*
b) ¿Es un sistema de estación central? *SI*
    i. ¿Está conectado a la sede de guardias de la instalación? *SI*
    ii. ¿Está conectado directamente a una sede fuera de la instalación propiamente dicha? ¿Es un servicio privado de protección? ¿es a la estación de policía? ¿es a la estación de bomberos? *SÍ, pero no está conectado a los bomberos.*

44. ¿El sistema está respaldado por guardias de alerta adecuadamente entrenados?

Sí, la alarma tiene un servicio de respuesta de eventos armado.

45. ¿Está desactivado el sistema de alarma de las áreas activas de las estructuras durante las horas de operación?

Sí, la alarma solo está activa de noche.

46. ¿Se prueba el sistema antes de activarlo desde períodos no operativos?

Sí, la alarma tiene sistema de auto diagnóstico.

47. ¿El sistema de alarma es inspeccionado regularmente?

Sí, viene incluido dentro del servicio de mantenimiento

48. ¿Es el sistema inviolable? ¿A prueba de la intemperie?

Sí, el intruso tendría que llegar hasta muy adentro para poder acceder al módulo de administración.

49. ¿Se ha previsto un sistema de alarma alternativo para su uso en caso de fallo del sistema primario?

No, si el sistema principal falla, no hay un sistema de respaldo.

50. ¿Existe una fuente de energía alternativa o independiente disponible para su uso en el sistema en caso de fallo de alimentación?

Sí, la alarma cuenta con sistema de batería independiente que le permite operar por un máximo de 2 días.

51. ¿La fuente de alimentación de emergencia está diseñada para cortar y operar automáticamente?

5.2.8 Lista de control de identificación y control del personal.

52. ¿Se utiliza una tarjeta de identificación o carné para identificar a todo el personal dentro de los confines de las áreas controladas?

Sí, todos los colaboradores tienen uno y es obligatorio portarlo de forma visible dentro de las instalaciones.

53. ¿El sistema de identificación y control incluye acuerdos? para lo siguiente:

a) Protección de componentes codificados o impresos de carnés y pases. *NO*
b) Designación de las distintas zonas que requieren medidas especiales de control. *NO*
c) Emisión controlada de los medios de identificación. *NO*

54. ¿Existen procedimientos por escrito para el método de identificación en el momento de entrar y salir del área controlada? ¿Se aplica tanto a los empleados como a los visitantes?

a) Detalles de dónde, cuándo y cómo se portarán las tarjetas de identificación. *NO, esa información se da de boca en boca.*
b) Procedimientos que seguir en caso de pérdida o daño a los medios de identificación. *NO, solo se repone.*

c) Procedimiento de recuperación e invalidación. *NO, solo se repone.*

55. Si se utiliza un sistema de intercambio de credenciales para cualquier área controlada, ¿el sistema proporciona:

a) ¿Comparación de credencial, pase y personal? *No aplica*
b) ¿Intercambio físico del pase para la credencial en el momento de la entrada y de la salida? *No aplica*
c) ¿La seguridad de las credenciales no está en uso? *No aplica*

56. ¿Se le proporciona una identificación especial al personal que requiere ingresar regularmente en áreas de diversos grados de seguridad?

No, no existe una clasificación de grados de seguridad,

57. El personal que requiera acceso infrecuente a una zona crítica y que no haya recibido una identificación de seguridad regular para esa zona, es tratado como "visitantes" y le es emitido:

a) ¿Una tarjeta de visitante o un pase? *No aplica*
b) ¿Un pase especial? *No aplica*

58. ¿Se requiere que todo el personal use la credencial de identificación de seguridad mientras está de servicio?

Sí.

59. ¿Los guardias de los puntos de control comparan las credenciales con los portadores tanto al entrar como al salir?

No, no se pudo constatar la presencia de este proceso.

60. ¿Se registran y controlan las credenciales mediante rigurosos procedimientos de rendición de cuentas?

No, no se pudo constatar la presencia de este proceso.

61. ¿Se reemplazan las credenciales perdidas por uno que lleva un número diferente o por otro que no es idéntico al que se pierde?

No, la identificación es la misma.

62. ¿Cuáles son los procedimientos relativos a las credenciales perdidas, dañadas y/u olvidadas?

Solo se reponen.

63. ¿Son fijadas las listas de las credenciales perdidas en los puntos del control de la guardia?

No. Como la empresa es pequeña, la recepcionista conoce al personal y es ella la que autoriza los accesos al edificio durante el día, el proceso de generación de dichas listas no se realiza.

64. ¿Hay credenciales de tal diseño y apariencia que permitan a los guardias y a otro personal reconocer rápida y positivamente las autorizaciones y limitaciones aplicables a los portadores?

Sí, se usa foto grande.

65. ¿Los procedimientos existentes aseguran la devolución de las credenciales de identificación al terminar el empleo?

No, al menos no fue posible determinar esa información en un documento escrito. Nótese que el gafete es solo para identificación y no proporciona acceso a ninguna parte.

66. ¿Qué tipo de credenciales se emiten a los empleados externos de contratistas que trabajan dentro de la instalación?

No se emiten este tipo de credenciales.

67. ¿Están todas las fases del sistema bajo supervisión y control de los oficiales de seguridad?

No.

68. ¿Se establece un procedimiento de escolta de visitantes?

Sí, pero es más por cortesía que por seguridad.

69. ¿Los guardias verifican los movimientos de los visitantes para asegurarse de que no entran en áreas para las que no tienen la autorización requerida?

No, los espacios restringidos están bajo llave.

70. ¿Se requiere que los visitantes muestren visiblemente la identificación en las prendas exteriores en todo momento mientras estén en áreas controladas?

No, no se maneja identificación para visitantes.

71. Cuando los visitantes salen de la instalación, ¿están obligados a entregar sus credenciales de identificación?

No, no se maneja identificación para visitantes.

72. ¿La hora de salida está registrada en el registro de visitantes?

Sí, la recepcionista lleva control de esa información en la recepción.

73. Si los visitantes indican una intención de volver más tarde, ¿se les permite conservar sus credenciales de identificación?

No, no se maneja identificación para visitantes.

74. ¿Qué procedimientos se invocan cuando no se devuelven los medios de identificación de visitantes antes de la salida del visitante?

No, no se maneja identificación para visitantes.

75. ¿Hay una recepción central?

a) Si es "sí", especifique las funciones. *Sí, se autorizan los accesos al edificio y se anuncia a los invitados.*

b) ¿Se realizan las funciones bajo la supervisión de un oficial de seguridad? *No.*

76. **¿A los proveedores, los comerciantes, los trabajadores de servicios públicos, los trabajadores de equipo especial, entre otros, se les emite un tipo de credencial distintivo o especial?**

No, solo se emite credenciales a los colaboradores internos.

77. **¿Qué medidas se emplean, además de la emisión de credenciales de identificación, para controlar el movimiento de personal de otras compañías de transporte que trabajan dentro del perímetro de la instalación?**

Ninguno.

78. **¿Es el oficial de seguridad el funcionario responsable de todos los aspectos del control de visitantes?**

El oficial y la recepcionista.

Anexo 3: Cuestionario para evaluar el conocimiento de los colaboradores de la edificadora.

CUESTIONARIO 1 **Objetivo:** Determinar el conocimiento de la gestión de la información de los colaboradores de la Edificadora Beta Marque con una X la opción que corresponda a su respuesta.		
Pregunta.	**SI**	**NO**
¿Cuánto tiene de laborar para edificadora Beta?		
¿Sabe usted si existe alguna política de seguridad en Beta?		
empresa?		
¿Tiene usted presente los riesgos asociados al manejo de los datos?		
¿Tiene usted claras sus funciones y responsabilidades dentro de la empresa?		
¿Conoce las implicaciones legales por concepto de robo y fraude de información?		
¿Sabe usted que es un acuerdo de confidencialidad?		
¿Firmó usted algún acuerdo de confidencialidad cuando ingreso a la empresa?		
¿Conoce términos tales como Malware, fishing o ingenieria social?		
¿Bloquea usted su equipo cuando tiene que alejarse de él?		
¿Recicla usted contraseñas en los diferentes sistemas en donde tiene acceso?		
¿Utiliza algún software para la gestión de sus contraseñas?		
¿Existe algún dispositivo para la destrucción de documentos?		
¿Destruye los documentos s confidenciales impresos que no necesita después de		
¿Le interesaría recibir boletines y capacitaciones sobre seguridad de la información?		
Elaborado por: ROBERTO BUJAN		
Aplicado por:		
Fecha:		

Figura 18 Cuestionario para los colaboradores de la Edificadora.

Fuente: Elaboración propia.