

Buenos Aires, 17 de noviembre de 2021

Sr. Matías Videla
Gerente General
Cencosud S.A.

Ref: Informe de Avance del protocolo de ciberseguridad

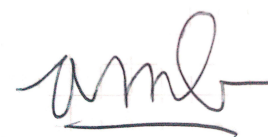
De mi consideración,

Por medio de la presente, tengo el agrado de dirigirme a Usted, a fin de enviarle el primer informe de avance del proyecto “Implementación del protocolo de ciberseguridad en Cencosud especializado en ransomware”.

En este informe se deja evidencia del trabajo realizado hasta la fecha actual sobre el protocolo propuesto en relación al sistema de seguridad informática de Cencosud en Argentina. Por consiguiente, se detalla brevemente el progreso de cada procedimiento.

Espero que la lectura de este informe sea de su agrado, desde ya agradezco su tiempo y atención. Quedo a su disposición ante cualquier comentario o consulta.

Atentamente,

A handwritten signature in dark ink, appearing to read 'amb', with a horizontal line underneath.

Ing. Augusto Borromeo
Gerente de capacitaciones de FutureLab

Informe de avance N°1: Implementación del protocolo de ciberseguridad en Cencosud especializado en ransomware

**Borromeo, Augusto; Calderón, Sergio; Coudannes, Pascual
Ercoli, Juan Martín; Mascioli, Bianca**

Contacto: futurelab_info@gmail.com

FutureLab, Av. L. N. Alem 1067, Piso 9, Buenos Aires

Índice

	Página
Introducción	1
Trabajo realizado (Borromeo, A.)	2
Trabajo realizado (Calderón, S.)	3
Trabajo realizado (Ercoli, J.)	4
Trabajo realizado (Coudannes, P.)	5
Trabajo realizado (Mascioli, B.)	6
Trabajo a realizar	7

Introducción

A raíz del ciberataque dirigido a Cencosud en el año 2020 y ante la falta de un plan de ciberseguridad por parte de la empresa, la misma no tuvo la capacidad de tomar las decisiones más óptimas registrándose así vulneraciones en la información de usuarios. Frente a esta problemática, se propuso el desarrollo de un protocolo de ciberseguridad especializado en Ransomware. La implementación del proyecto tiene como fin otorgar a Cencosud un plan de control de mitigación y prevención de futuros ciberataques.

En este informe se explican las actividades realizadas durante los primeros dos meses, es decir la mitad del tiempo total estipulado en el cronograma. Debido a que existen tareas que se pueden realizar en simultáneo, se describe cuáles etapas concierne al tiempo transcurrido en los procedimientos de capacitaciones, revisiones, protocolos y optimizaciones. Finalmente, también se especifican los procesos programados y pendientes de realización hasta la culminación del proyecto.

Trabajo realizado (Borromeo, A.)

Relacionado a las capacitaciones de marketing se realizaron las capacitaciones propias de sus fundamentos. En ellas se abarcaron aspectos como el público objetivo, métricas, objetivos de marketing, herramientas, como reaccionar en las redes sociales y con los clientes cuando suceden vulnerabilidades en ciberseguridad, entre otros. Los empleados que realizaron el curso tuvieron buenos resultados en el examen final. A continuación se presenta una imagen luego de haber recibido los certificados:



Figura 1. Empleados de Cencosud en el curso de capacitación de fundamentos del marketing

Por otro lado, junto a los gerentes y empleados que aprobaron la evaluación, se determinó el público objetivo de la empresa y cuales son sus principales metas a mediano y largo plazo respecto al mismo. Se establecieron metas de usuarios, indicadores, porcentaje de fidelización de clientes y un plan de modificación en la imagen y voz de marca. Finalmente todo aquello quedó registrado en un documento compartido de la empresa y se encuentra disponible para elegir las herramientas más óptimas.

Trabajo realizado (Calderón, S.)

En la primera etapa del proyecto se realizó el estudio exhaustivo de la información existente en el sistema de Cencosud y se clasificó la misma según la región geográfica y el supermercado (Jumbo, Disco, Vea, Easy), de modo de prepararlos para su distribución. Se encontró que, como era esperado, el mayor porcentaje de los clientes y actividad comercial de Argentina se encuentra en la ciudad de Buenos Aires y la respectiva área metropolitana.

En simultáneo, se comenzó con la instalación física de los nuevos servidores rack, correspondiente a la etapa de “Implementación inicial”, de acuerdo al cronograma previsto. Previamente se compraron los equipos y los accesorios necesarios para su funcionamiento: cables UTP, rack murales de 19”, cerraduras y discos duros, en una cantidad proporcional al presupuesto otorgado para la realización del proyecto. Se armaron los bastidores para la colocación de los equipos dentro de armarios refrigerados, y luego se realizó el cableado a la red WAN de la empresa, como se constata en la figura a continuación:



Figura 2. Nuevos servidores rack instalados en sus armarios correspondientes.

Luego del correcto montaje de los servidores, se realizó la instalación y activación del sistema operativo en cada uno de los equipos, como así también los programas de autenticación y realización de modificaciones y consultas en las bases de datos.

La realización de las tareas mencionadas anteriormente se cumplieron en los plazos establecidos. Una vez terminadas ambas etapas, se realizó la distribución de la información recolectada, para lo cual se almacenaron los datos en los servidores correspondientes. Para el momento de realización de este informe, aún no se comenzó la implementación del sistema automatizado de gestión de claves para la información que debe protegerse en el sistema.

Trabajo realizado (Ercoli, J.)

De acuerdo a la primer etapa del proyecto:

Se comenzó con la etapa del diseño y especificaciones del protocolo informático (ver Figura 3) enfocado a malwares ransomware, proceso en el cual se analizó toda la información recopilada, se elaboró una estructura protocolar y se diseñó un borrador con las secciones y sub-secciones constitutivas del protocolo y las implicancias de cada una.

Las secciones que se definieron son: propósito del protocolo, introducción, implementación, normas específicas de ciberseguridad, acciones a tomar. Se escribieron las primeras 4 secciones y se dejó para las siguientes etapas las sub-secciones de la sección ‘acciones a tomar’. También se agregó un anexo didáctico que invita al lector a investigar más acerca de la temática de ciberseguridad.



Figura 3. Grupo de trabajo en la planificación del protocolo (etapa 1).

Una vez definidas acordemente las secciones se procedió con la segunda etapa donde se definió la primer sub-sección de ‘acciones a tomar’ llamada ‘prevención de un ataque ransomware’ donde se establecieron las medidas y recomendaciones que debe tomar el personal para prevenir un posible ataque de ransomware, al final de la sección se colocaron técnicas que pueden resultar útiles tomar previo a un ciberataque.

Gracias al eficaz trabajo del equipo de informáticos se logró cumplir con la etapa 2 antes del tiempo estipulado en el cronograma de actividades. El sueldo del equipo cumplió con lo estipulado en el presupuesto de la propuesta.

Trabajo realizado (Coudannes, P.)

En la primera etapa “diagnóstico de conocimientos del personal”, se realizó una serie de encuestas virtuales. Las mismas fueron enviadas vía mail a todo el personal. Se corrigieron y clasificaron los resultados dependiendo los conocimientos. Dejando tres grupos: básico, intermedio y avanzado.

Continuando con la siguiente etapa “planificación”, se confeccionó el cronograma de actividades para las próximas tres semanas (etapa 3). El calendario se ajustó a los horarios de los trabajadores. También se preparó las diferentes diapositivas de las presentaciones. Se consiguió un espacio para poder hacer las capacitaciones, junto con una manta blanca y el proyector.

Durante las actividades de “ejecución” se realizaron las respectivas charlas. A medida que avanzaron los días, fueron más técnicas y exigentes. La primera semana hubo dos charlas para aquellos que tenían conocimientos básicos. La segunda semana se realizó una capacitación para las personas de nivel básico e intermedio. Y la última semana hubo dos cursos para todos los niveles. Se usó una habitación junto con el proyector y la manta blanca.



Figura 4. Capacitación de la etapa 3.

Como última parte se realizó la “evaluación”, consistió en un examen final con todos los contenidos dados en las charlas. Los resultados fueron entregados a los gerentes. Para la finalización de la actividades se contrató a un catering.

Trabajo realizado (Mascioli, B.)

Durante los primeros dos meses se finalizaron las primeras dos etapas del protocolo de revisión y actualización de seguridad periódica de los equipos y servidores de la empresa y se comenzó la tercera etapa. Durante la primera etapa se realizó el **diagnóstico de seguridad de los equipos y servidores**. Para realizar este diagnóstico se revisaron los equipos y servidores informáticos de la empresa con la finalidad de obtener en qué estado se encontraban y que falencias de seguridad presentaban. Luego de realizar la revisión se procedió a categorizar el estado de los aspectos más importantes relacionados a la seguridad informática. Estos aspectos fueron evaluados en 5 niveles, desde el más deficiente (nivel 1) al más eficiente (nivel 5), como se muestra a continuación en la Tabla 1.

Tabla 1. Diagnóstico de seguridad de los equipos de Cencosud

DIAGNÓSTICO	ESTADO				
Sistemas de autenticación.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Técnicas de encriptación.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Software de eliminación de virus.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Firewall.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Copias de seguridad.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Conectividad de los equipos.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

En la segunda etapa, se realizó **el diseño de la actualización de los equipos y servidores** para resolver las falencias encontradas a partir de los datos recolectados en la primera etapa. Se hizo especial énfasis en diseñar una solución para los aspectos con menor nivel como por ejemplo, realizar copias de seguridad, actualizar el Firewall existente, y reforzar la encriptación de datos. Por último se comenzó a desarrollar la tercera etapa que consiste en **la ejecución del plan diseñado**, empezando así con las instalaciones y actualizaciones del protocolo.

Para la realización de las etapas se contrataron tres profesionales quienes son quienes estarán a cargo de todas las etapas del protocolo. Este grupo de profesionales está conformado por un experto en ciberseguridad, un analista en sistemas, y un ingeniero en computación. El sueldo de estos profesionales es el mismo al estipulado en el presupuesto. Hasta el momento las etapas fueron realizadas de acuerdo al cronograma antes establecido.

Trabajo a realizar

A continuación se detallarán las próximas tareas cuya realización se concretarán en las próximas etapas:

Se analizarán qué herramientas de medición de marketing son las más óptimas para los objetivos y público objetivo que se eligieron. Entre aquellas herramientas se incluirán dashboards, programas de software y manejos de redes sociales. Luego se montotizará a la empresa en cuanto a practicidad e implementación de los conocimientos.

Para el procedimiento de optimización del sistema de bases de datos, se realizará la implementación del gestor automatizado de claves para culminar la etapa de distribución de los datos. Luego, se crearán los perfiles de usuario con sus respectivos permisos y se realizarán pruebas exhaustivas de verificación para asegurar el funcionamiento del sistema.

Respecto al apartado del protocolo resta la etapa de definiciones de la sección de ‘mitigación de un ataque ransomware’ donde se establecerán las medidas y recomendaciones que debe tomar el personal para mitigar un ataque de ransomware. Se concluirá con la última etapa en la que se realizará un análisis y revisión de cada subproceso de la implementación protocolar cuya duración se espera que sea de un mes.

En relación al protocolo de revisión de los equipos, se estima que en las próximas dos semanas se finalizará con la ejecución del plan diseñado. Luego se procederá con la última etapa que involucra la evaluación del plan ya ejecutado donde se analizará si el mismo funciona de forma correcta. De lo contrario, se deberá diseñar uno nuevo donde se busque otra forma de resolver los problemas de seguridad informáticos.

Con respecto a la “realización de cursos y charlas personalizadas” sus actividades finalizaron en el tiempo transcurrido.