Buenos Aires, 5 de noviembre de 2021

Sr. Matías Videla
Gerente General
Cencosud S.A.

Ref: Proyecto de protocolo de ciberseguridad

De mi consideración,

Por medio de la presente, tengo el agrado de dirigirme a Usted, a fin de enviarle el Plan de Proyecto “Implementación de un protocolo de ciberseguridad en Cencosud especializado en ransomware”.

En dicha propuesta se sugiere la aplicación de medidas sobre el sistema de Cencosud en Argentina, así como también al personal, planteando la incorporación de protocolos, capacitaciones y revisiones periódicas, junto al rediseño de un sistema eficiente y seguro de datos, para evitar nuevos daños por ciberataques a la empresa.

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,

Ing. Sergio Calderón
Gerente de Desarrollo de FutureLab

Proyecto para la implementación de un protocolo de ciberseguridad en Cencosud especializado en ransomware

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

Contacto: futurelab_info@gmail.com

Future Lab, Av. L. N. Alem 1067, Piso 9, Buenos Aires

Índice

Página

Resumen

En noviembre de 2020, se produjo un ciberataque importante al sistema del consorcio empresarial Cencosud en Argentina, el cual tuvo repercusiones económicas tanto para sus clientes, por el filtrado masivo de sus datos privados, como así también para la empresa, por su imagen corporativa afectada por las penalizaciones judiciales llevadas a cabo en 2021. A raíz de este hecho, la siguiente propuesta presentará una serie amplia de medidas de manera detallada para la implementación de un protocolo de ciberseguridad en la empresa Cencosud en Argentina, enfocado principalmente en ransomware, que aplicarán tanto sobre los equipos informáticos como así también a los empleados. Su correcta realización aumentaría la protección de todo el sistema y el conocimiento del personal en este ámbito. De esta manera se podrán evitar nuevos ataques informáticos de características similares.

Palabras clave

Base de datos, capacitación, marketing, protocolo de seguridad, revisión periódica.

Introducción

El consorcio empresarial Cencosud fue víctima de un ciberataque por ransomware en noviembre de 2020, en el cual se filtró una gran cantidad de datos importantes. A raíz de este hecho, los atacantes difundieron la información para su libre acceso. Esto produce un daño potencial a los clientes y la imagen empresarial, por ejemplo, hay casos de *spam* luego de efectuar compras online, principalmente en Easy Argentina, y también hubo sanciones.

Los cambios ocasionados por la pandemia han acelerado la digitalización de los procesos, el flujo de datos informáticos ha aumentado (Firstbrook, 2020). Por lo tanto, implementar medidas de ciberseguridad es esencial para las organizaciones, y para llevarlas a cabo se requiere contar con herramientas tecnológicas (Thomson Reuters, 2020).

La propuesta presentada tiene como propósito resolver las deficiencias de seguridad en el sistema de la empresa Cencosud. De esta manera, para cumplir con el objetivo deseado y así reforzar la protección de la información de la empresa se plantean distintos enfoques, entre ellos la incorporación de protocolos, capacitaciones y revisiones periódicas, junto al rediseño de un sistema eficiente y seguro de datos.

Fundamento

Cencosud es una organización que está compuesta por varias importantes y tiene injerencia en 5 países de América del Sur: Chile, Argentina, Brasil, Perú y Colombia; de los cuales en el primero es la empresa líder y en el segundo representa el 21% del sector supermercadista con Jumbo, Disco y Vea. El conjunto de datos de todos los clientes, en adición con la información de tarjetas de crédito, representa un gran volumen de información que debe preservarse adecuadamente, con todos los requerimientos que sean necesarios.

Sin embargo, dicha información se encuentra concentrada en un único sistema, cuya seguridad se ha mostrado poco eficiente en el ataque producido por el ransomware Egregor, a tal punto que tuvo repercusiones en los dos países principales en simultáneo.

La propuesta para solucionar esta problemática consta de 3 partes:

1. Capacitación del personal sobre ciberseguridad.
2. Implementación de protocolos y revisiones.
3. Diseño y puesta en marcha de una base de datos distribuida.

La finalidad de la primera parte es brindar conocimiento específico a los empleados involucrados en la manipulación de los datos del sistema, focalizando en la navegación segura y ransomware, para evitar la descarga de malware y su propagación descontrolada.

Por otro lado, la segunda sección abarca protocolos de mitigación y encriptación, cuya implementación permite la protección de los datos y reducción de daños en equipos involucrados de la empresa. En adición, los chequeos periódicos de las funciones de seguridad garantizarán que el sistema esté actualizado a fin de prevenir nuevos ataques.

Respecto al diseño de un sistema de base de datos distribuida, es una metodología que ofrece fiabilidad, eficiencia de tráfico y robustez, al no existir un único sistema donde todos los datos son directamente accesibles. En el extremo caso de producirse un ciberataque, no será posible realizar un filtrado masivo a diferencia de lo sucedido en 2020.

En caso de no aprobarse la realización del proyecto, el sistema de Cencosud permanecerá vulnerable a futuros ciberataques, los cuales aumentan en cantidad e ingenio cada año, ocasionando más pérdidas económicas por el pago de rescate de datos cifrados, o bien, por las multas al permitir la distribución de la información de los clientes, que además de resultar perjudicados, optarán por realizar sus compras en tiendas de la competencia.

Implementación del protocolo informático (Ercoli, J.)

El proceso para la definición e implementación de un protocolo informático con el objetivo de mitigar ciberataques con ransomware con destino de ataque a empresas que manejan datos de alta importancia se puede observar en la Figura 1 divido en 4 subprocesos: diseño y especificaciones del protocolo, definiciones de la sección de prevención, definiciones de la sección de mitigación, análisis y revisión de cada subproceso.

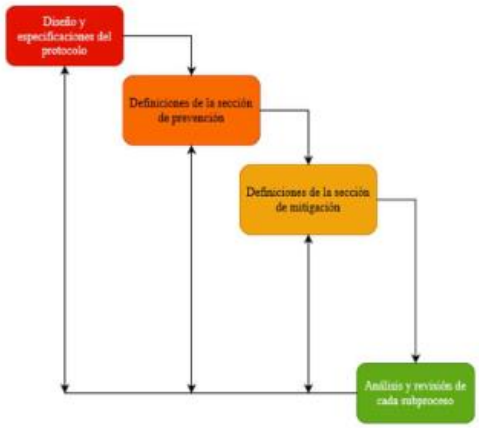


Figura 1 Diagrama de flujo para el diseño del protocolo informático

En la etapa de diseño y especificaciones del protocolo se crea un borrador o diseño preliminar con las secciones del protocolo y se delimitan las implicancias que tiene cada sección, el diseño en este caso está dirigido a un protocolo enfocado a prevenir ransomwares.

Posteriormente se realizarán definiciones para cada sección:

Sección de prevención: se detallarán las recomendaciones y medidas a tomar para prevenir la infección por ransomware a un dispositivo de la empresa, como por ejemplo la realización de backups regulares, técnicas para evitar propagaciones del virus en la red, técnicas para evitar que los virus sean ejecutados y preparaciones para un ataque.

Sección de mitigación: se detallarán las recomendaciones y medidas a tomar para mitigar los daños a dispositivos que ya fueron infectados, como por ejemplo técnicas para analizar pérdidas de datos, primeros pasos a seguir ante un ciberataque y cómo eliminar remanentes del virus.

La etapa de análisis y revisión de cada subproceso consiste en como su nombre lo indica, realizar verificaciones a cada artículo pertinente a cada sección con el fin de eliminar toda ambigüedad y mejorar la redacción de cada uno para que todo el personal sea capaz de interpretar correctamente el protocolo.

Optimización de las bases de datos (Calderón, S.)

La implementación de un sistema de gestión de base de datos robusto y eficaz es un proceso que consta de 3 partes principales, como puede observarse en la Figura 2: la instalación física de los servidores, la distribución de los datos y el control de la actividad.

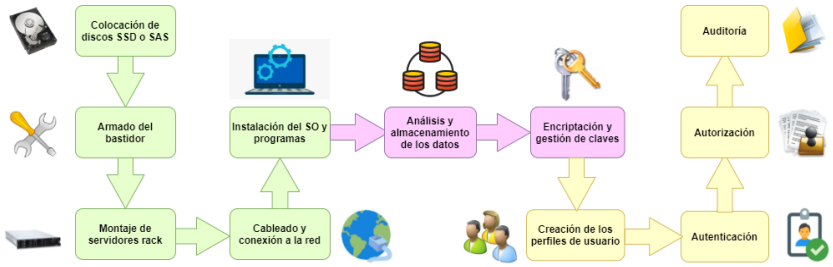


Figura 2. Diagrama de flujo del proceso de optimización del sistema de datos, coloreado por parte

En la instalación, los discos duros se colocan en los servidores según su utilización, destinando los tipos SSD[1] para e-commerce, y SAS[2] para almacenamiento permanente. El bastidor se arma en el lugar de trabajo, y los servidores *rack* (ver glosario) se montan en dicho soporte. Luego de la colocación de los equipos, se realiza el cableado, se conectan los mismos a la red y se instala el sistema operativo, junto con todos los programas que sean necesarios.

Para la distribución de los datos, la información se analiza y clasifica según su uso, tienda y privacidad, para su almacenamiento en el disco adecuado. Los datos sensibles se protegen mediante encriptación, para lo cual se realiza un cifrado. Un sistema automatizado administra las claves (ver Apéndice A), lo cual permite que las mismas sean seguras.

El control y registro de la actividad es un factor clave. En primer lugar, se crean perfiles de usuario de acuerdo al sector de la empresa, de modo que las personas se identifiquen mediante el inicio de sesión. El sistema operativo autoriza el acceso a los datos según los permisos de cada rol. Por último, el servidor lleva un registro diario de todas las consultas y modificaciones, también denominado auditoría.

Resulta importante que, luego de la puesta en funcionamiento del servicio, se mantenga el reparto de la nueva información según los criterios anteriormente mencionados, favoreciendo a las operaciones locales y las futuras revisiones de mantenimiento preventivo.

[1] Disco de estado sólido, caracterizado por su gran velocidad en comparación a los discos rígidos tradicionales.
[2] Serial Attached SCSI, caracterizado por su rendimiento y fiabilidad, esencial para la integridad de los datos.

Realización de cursos y charlas personalizadas (Coudannes, P.)

El procedimiento consiste en la realización de charlas y capacitaciones personalizadas dependiendo las necesidades y los conocimientos del personal. A continuación, se describirán los procesos para la realización de la solución, estos se pueden ver en el siguiente diagrama (Fig. 3).

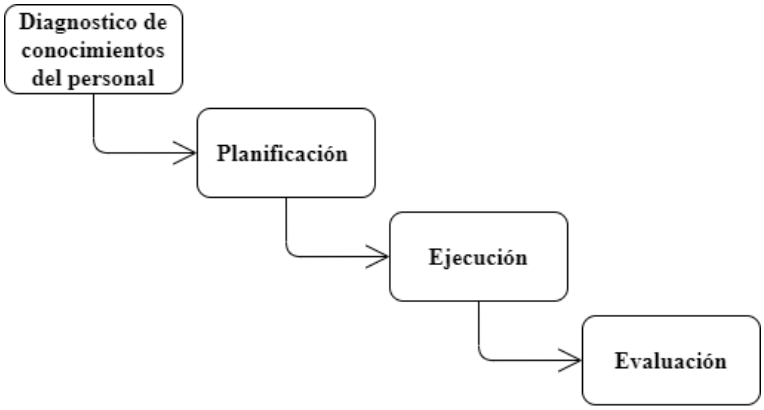


Figura 3: Diagrama de flujo de procedimientos.

Diagnóstico de conocimientos del personal: La primera etapa consiste en realizar test rápidos a través de encuestas o mini evaluaciones a los distintos tipos de personal, para tener noción de sus conocimientos. Con esto se tiene un pantallazo para la personalización de las charlas con el objetivo de que se saque el máximo provecho y los empleados sientan motivación para participar de las mismas. Los criterios de exigencia están basados en el puesto de trabajo y las responsabilidades del personal. Se necesitará confeccionar las encuestas de forma física o digital.

Planificación: Con la información obtenida se confecciona un cronograma de 21 días para las charlas y/o capacitaciones. Se administrarán desde las más básicas, hasta los temas más complejos. Los horarios se ajustarán a los horarios de trabajo y de ser necesario se pueden repetir en distintos turnos. La idea es presentar esta parte en tiempo y forma para que todos puedan acomodar sus horarios para la participación y el cumplimiento de las mismas. Simplemente se necesitarán los horarios en los que trabaja la empresa y su disponibilidad para la participación de la mayoría del personal.

Ejecución: En esta parte es donde se realizarán las charlas y capacitaciones correspondientes al cronograma confeccionado en la etapa de “Planificación”. Donde se empezará con el personal que tenga solo los conocimientos básicos. A medida que se avance con el cronograma se sumarán los demás integrantes. Se buscarán espacios donde realizar las charlas y las capacitaciones. También un proyector y una pizarra para plasmar las diapositivas

o ideas que surjan respectivamente. Para más detalles sobre la organización y ejecución de las capacitaciones (ver Apéndice B).

Evaluación: Como última fase se realizará una evaluación donde se verificará que el personal está capacitado con el fin de demostrar que se adquirieron los conocimientos. También se dará lugar al personal y a los gerentes para una devolución sobre las jornadas de capacitación. Se necesitarán varias jornadas en la que se pueda evaluar. Y confeccionar la evaluación.

Capacitación al personal sobre Marketing digital (Borromeo A.)

En este proceso se busca formar un equipo de marketing estable y eficiente a la hora de tomar decisiones de este rubro en la empresa.

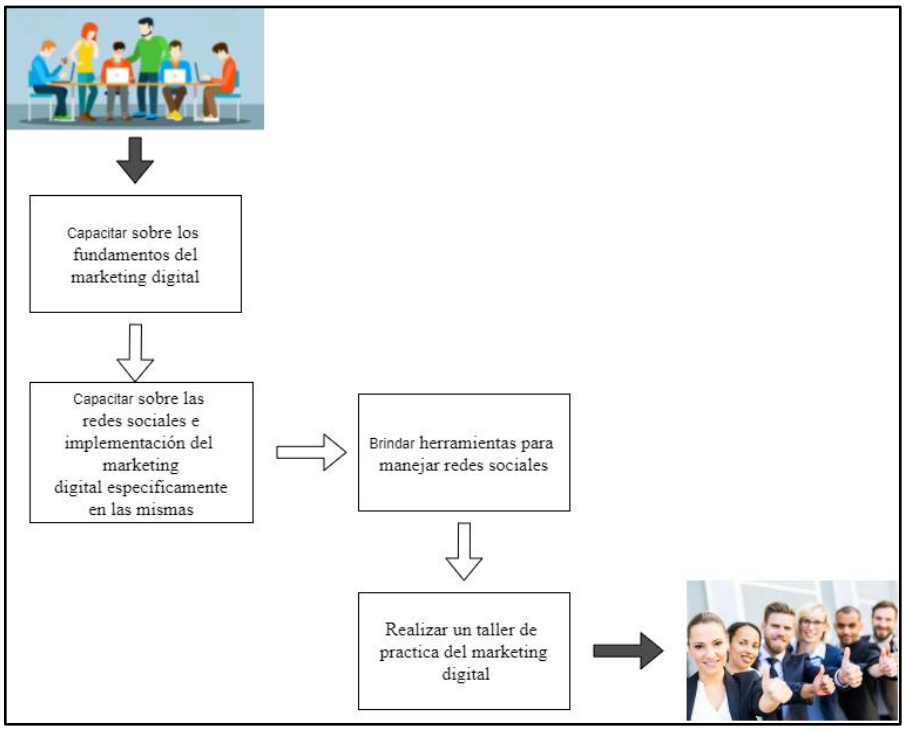


Figura 4. Diagrama de flujo del proceso de capacitación de marketing digital.

Detallamos cada uno de los procesos:

Capacitar sobre los fundamentos del marketing digital: En este aspecto se abordarán los principios del marketing digital. Qué es el público objetivo, cómo identificarlo, que son los OKR y KPI, canales de distribución, tipos de equipos, etc..

Capacitar sobre las redes sociales e implementación del marketing digital específicamente en las mismas: En esta sección se ilustra la aplicación del marketing digital en las redes sociales. Se definen estas últimas. Analizamos las estrategias principales del marketing digital en las redes sociales. Qué equipos son efectivos en las redes sociales, etc.

Brindar herramientas para manejar redes sociales: Se da a conocer herramientas para medir interacciones, automatización de publicaciones, creación de campañas de marketing, programas de diseño, etc.

Realizar un taller de práctica del marketing digital: Finalmente en este apartado se integra lo visto anteriormente en un taller de práctica para evaluar los conocimientos adquiridos y poder aplicarlos en la empresa.

Revisión y actualización de seguridad periódica de los equipos y servidores de la empresa (Mascioli, Bianca)

Con los avances de la tecnología se incrementan constantemente las maneras de realizar daño a los equipos y servidores de la empresa con el fin de obtener sus datos. Es por ello que es necesario ser consciente de estas amenazas y prever la forma de evitarlas o mitigarlas.

De esta forma el siguiente procedimiento tiene como objetivo diseñar un protocolo de revisión y actualización de seguridad periódico de los equipos y servidores de la empresa. El procedimiento (Fig. 5) deberá ser periódico, es decir que este procedimiento se deberá aplicar en la empresa cada un periodo establecido (inicialmente cada 6 meses), ya que como dijimos anteriormente las amenazas se multiplican rápidamente y los sistemas de protección deben ser actualizados continuamente.

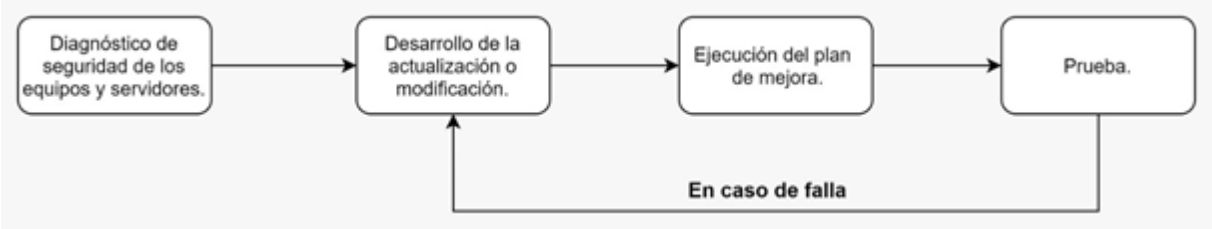


Figura 5. Diagrama de flujo del proceso de revisión y actualización de seguridad.

Diagnóstico de seguridad de los equipos y servidores: la primera etapa consiste en que los equipos y servidores de la empresa sean revisados por un grupo capacitado de empleados de la empresa. En esta revisión se obtendrán datos sobre qué falencias de seguridad y que sistemas de defensa tienen los equipos y servidores.

Desarrollo de la actualización o modificación: en esta etapa se decide cómo resolver las falencias de seguridad existentes. Se pueden actualizar los sistemas de defensas preexistentes como firewall[3], antivirus, entre otros. O bien se puede buscar un reemplazo de esa actual forma de defensa ineficaz.

Ejecución del plan de mejora: en esta etapa se pone en marcha el plan de mejora. La instalación o actualización deberá ser realizada por los mismos empleados que hicieron el diagnóstico al principio.

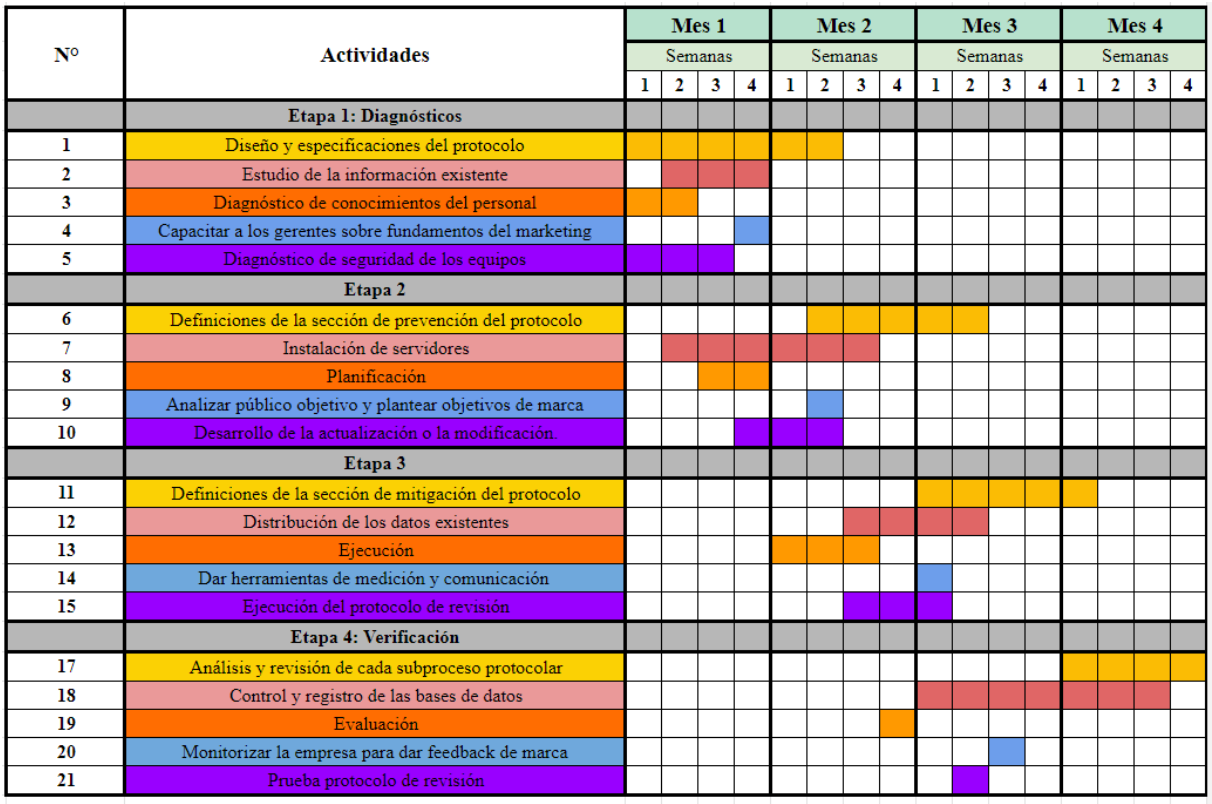
[3] Un firewall proporciona un modo de filtrar la información que se comunica a través de la conexión de red.

Prueba: en esta última etapa se analiza si el plan ejecutado funciona de forma correcta. De lo contrario, se vuelve a la etapa de desarrollo donde se buscará otra forma de resolver los problemas de seguridad. Esta etapa también es realizada por el mismo equipo de empleados capacitados.

Con este protocolo se logra aumentar la confianza en los sistemas de seguridad de los equipos y servidores de la empresa y se disminuye la posibilidad de que estos mismos sean dañados.

Cronograma

El cronograma de actividades (Fig. 6) muestra cómo todos los procedimientos se deben llevar a cabo a lo largo de dieciséis semanas, desarrollando tareas en simultáneo.



N°	Actividades	Mes 1				Mes 2				Mes 3				Mes 4			
		Semanas				Semanas				Semanas				Semanas			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	Etapa 1: Diagnósticos																
1	Diseño y especificaciones del protocolo																
2	Estudio de la información existente																
3	Diagnóstico de conocimientos del personal																
4	Capacitar a los gerentes sobre fundamentos del marketing																
5	Diagnóstico de seguridad de los equipos																
	Etapa 2																
6	Definiciones de la sección de prevención del protocolo																
7	Instalación de servidores																
8	Planificación																
9	Analizar público objetivo y plantear objetivos de marca																
10	Desarrollo de la actualización o la modificación.																
	Etapa 3																
11	Definiciones de la sección de mitigación del protocolo																
12	Distribución de los datos existentes																
13	Ejecución																
14	Dar herramientas de medición y comunicación																
15	Ejecución del protocolo de revisión																
	Etapa 4: Verificación																
17	Análisis y revisión de cada subproceso protocolar																
18	Control y registro de las bases de datos																
19	Evaluación																
20	Monitorizar la empresa para dar feedback de marca																
21	Prueba protocolo de revisión																

Figura 6. Cronograma de actividades.

Los procesos se indican por color:

	Proceso para la implementación del protocolo informático (Ercoli, Juan M.)
	Proceso de optimización de las bases de datos (Calderón, Sergio)
	Proceso de solución mediante cursos y charlas personalizadas (Coudannes, Pascual)
	Proceso de capacitación al personal sobre Marketing digital (Borromeo Augusto)
	Proceso de revisión y actualización de seguridad periódico de los equipos y servidores de la empresa. (Mascioli, Bianca)

Como puede observarse, solo se muestra la duración de los procesos por etapas. No se detallan los subprocesos ni su extensión. Cualquier actividad está abierta a modificaciones dependiendo las circunstancias. Pueden comprimir o extender su longitud, y en caso de ser necesario cambiar su desarrollo.

Personal

En la Tabla 1 se muestran todos los recursos humanos necesarios para la realización de la propuesta, detallando la cantidad de personal de cada oficio y la tarea que tendrá asignada.

Tabla 1. Personal requerido para la propuesta

Item	Puesto	Cantidad	Tarea
1	Ingeniero en Computación	3	Protocolo de revisión de los equipos y servidores. Estudio de los datos, automatización y testeo del sistema Supervisión para el diseño, especificaciones y definiciones del protocolo.
2	Técnicos de sistemas	5	Diseño, especificaciones y definiciones del protocolo Puesta en funcionamiento de los servidores
3	Trabajador Social	1	Diagnostico de conocimientos del personal. Planificacion. Ejecucion. Evaluacion
5	Profesores de marketing digital	3	Su responsabilidad dentro de la propuesta es capacitar al futuro equipo de marketing de la empresa.
6	Experto en Ciberseguridad	2	Protocolo de revisión de los equipos y servidores.
7	Analista de sistemas	1	Protocolo de revisión de los equipos y servidores. Identificación de los tipos de usuarios y sus permisos
9	Experto en comunicación protocolar	1	Analisis y revisión del protocolo
10	Operarios	20	Instalación de los servidores y testeo del sistema

Presupuesto

En la Tabla 2, se muestra de manera detallada el presupuesto completo, compuesto en primer lugar por los gastos de recursos humanos, y luego por compra de materiales y equipos.

Tabla 2. Presupuesto requerido para la propuesta

Ítem	Descripción	Unidad	Cantidad	Costo Unitario ($)	Costo total ($)
1	**Costo Personal**				
1.1	Ingeniero en Computación	DH	3	100,000	300,000
1.2	Técnicos de sistemas	DH	5	50,000	250,000
1.3	Trabajador Social	DH	1	36,000	36,000
1.4	Profesores de marketing digital	DH	3	40,000	120,000
1.5	Experto en Ciberseguridad	DH	2	70,000	140,000
1.6	Analista de sistemas	DH	1	70,000	70,000
1.7	Experto en comunicación protocolar	DH	1	70,000	70,000
1.8	Operarios	DH	20	40,000	800,000
2	**Materiales**				
2.1	Proyector	Unidad	2	12,000	24,000
2.2	Antivirus empresarial	Unidad	1	20,000	20,000
2.3	Firewall empresarial	Unidad	1	95,000	95,000
2.4	Servidor tipo rack	Unidad	8	230,000	1,840,000
2.5	Rack Mural 6U 19"	Unidad	2	12,000	24,000
2.6	Disco Duro SSD 2 TB	Unidad	3	7,000	21,000
2.7	Disco Duro SAS 1 TB	Unidad	5	28,000	140,000
2.8	Cable de Red UTP	m	500	30	15,000
2.9	Software de marketing digital	Unidad	3	9,000	27,000
3	**Gastos varios**				
3.1	Catering	Unidad	1	39,500	39,500
Total					4,031,500

Discusión

El ciberataque de Cencosud involucró consecuencias negativas tanto para la empresa como para sus clientes. Este ataque ocurrió porque la empresa no le dio la importancia necesaria a la amenaza y no protegió sus sistemas informáticos de la forma correcta, comprometiendo así información valiosa de los usuarios. Este ataque puede ser la antesala de muchísimos otros ataques informáticos si no se toman las medidas pertinentes en el ámbito de la ciberseguridad empresarial. Esto exige un planteo de nuevos modelos de seguridad cuyos fundamentos se encuentran a partir de:

La capacitación del personal que mejorará las capacidades intelectuales de cara la prevención de futuros ciberataques. Los procesos serán más eficientes ya que aumentará la seguridad de los trabajadores a la hora de manipular el equipamiento.

La capacitación de aspectos del marketing digital con el fin de manejar futuras crisis, independientemente de si se trata de ciberataques, en las redes sociales.

La implementación de un protocolo informático que guíe rigurosamente al personal acerca de cómo evitar ciberataques y, en caso de sufrirlos, cómo mitigarlos. Recordemos que las principales causas de recibir un ciberataque son por fallas humanas. Este sistema protocolar permitirá a la empresa evitar recibir daños graves respecto a los aspectos de los datos, reputación, venta, marketing y económicos.

La implementación de un sistema de gestión de base de datos robusto y eficaz que resultará en sistemas informáticos cuyo manejo de datos será realizado con más seguridad y eficiencia.

La implementación de un protocolo de revisión periódico de equipos y servicios de la empresa que hará posible disminuir el nivel de riesgo de forma significativa y con ello la materialización de las amenazas y la reducción su impacto sin necesidad de realizar elevadas inversiones ni contar con una gran estructura de personal. De esta manera con un protocolo que evalúe el estado actual de seguridad de los equipos y verifique de manera crítica la efectividad de los controles existentes, se podrán actualizar y proteger los equipos de la empresa de manera que puedan brindar un funcionamiento adecuado. Los resultados de esta evaluación periódica ayudarán a orientar y a determinar una apropiada acción gerencial y las prioridades para gestionar los riesgos de seguridad informática, así como la implementación de los controles seleccionados para protegerse.

Bibliografía

- Firstbrook, P. (22 de junio de 2020): Gartner Top 9 Security and Risk Trends for 2020. Disponible en Internet: https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020. 16 de octubre de 2021.

- Thomson Reuters (19 de agosto de 2020): Importancia de la ciberseguridad en las empresas. Disponible en Internet: https://www.thomsonreuters.com.ar/es/soluciones-fiscales-contables-gestion/blog-empresas/cual-es-la-importancia-de-la-ciberseguridad-para-las-empresas.html. 17 de octubre de 2021.

- Actualidadrt (19 octubre de 2021): Un multimillonario israelí y experto en ciberseguridad advierte que el rápido crecimiento de la industria podría causar una burbuja. Disponible en Internet: https://actualidad.rt.com/actualidad/407622-experto-ciberseguridad-advierte-rapido-crecimiento. 20 de octubre de 2021.

Glosario

- Disco SAS: tipo de disco de interfaz Serial Attached SCSI, caracterizado por su rendimiento y fiabilidad, esencial para la integridad de los datos.

- Disco SSD: disco de estado sólido, caracterizado por su gran velocidad de operación en comparación a los discos rígidos tradicionales.

- Servidor rack: computadoras compactas, con un ancho estándar de 19'' y un alto también estandarizado medido en unidades U, diseñadas para alojarse en armarios rack (armarios informáticos). A diferencia de los equipos de torre, no están pensados para ser situados sobre un escritorio, sino que son indicados cuando se necesita utilizar varios equipos en una misma instalación, apilados cada uno por encima del otro.

Apéndice A

Software gestor de claves

Un gestor de claves o contraseñas es un servicio que permite generar y administrar las credenciales de acceso para archivos cifrados y sitios web, todas distintas por recomendación. Si se reitera en el uso de una misma contraseña, se expone a la empresa a una fuerte vulnerabilidad de seguridad, ya que un tercero que la obtenga muy probablemente intentará y conseguirá acceder a los demás sitios con la misma clave.

Mediante la utilización del gestor, se generan claves totalmente aleatorias y con una longitud razonable, como se observa en la Figura A1, de modo que no sea descifrable a fuerza bruta[4]. El usuario no necesita recordar cada una de las contraseñas, evitando que el mismo las escriba en algún medio, lo cual también representaría un riesgo potencial de seguridad.

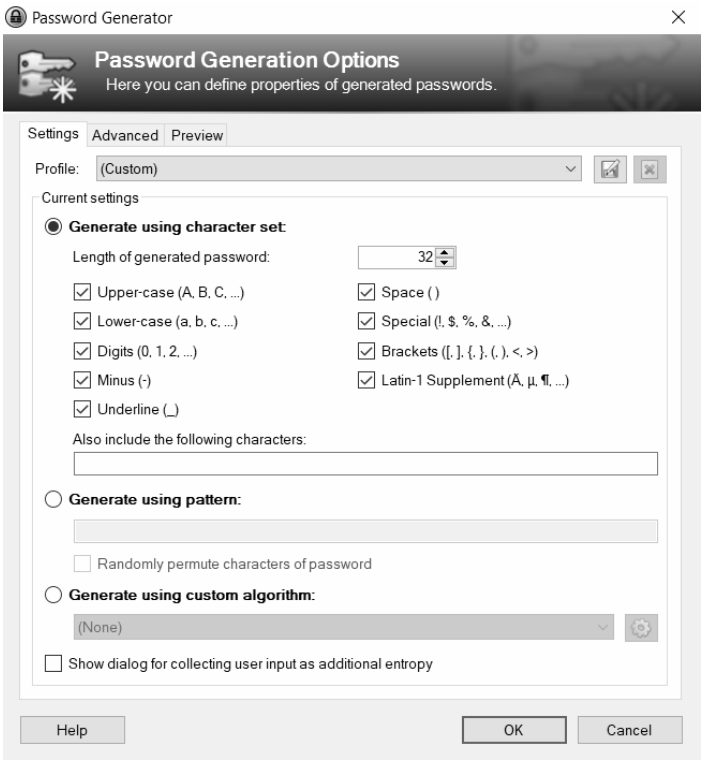


Figura A1. Interfaz de generación personalizada de contraseñas del software gestor.

Se puede distinguir entre dos tipos de clave de cifrado: simétrica y asimétrica. En la primera opción, se utiliza una misma clave para cifrar y descifrar datos entre el emisor y receptor, por ende, ambas partes deben comunicarse previamente y deben tener acceso a la clave. El remitente cifra un documento utilizando la clave, lo envía al destinatario, y éste lo

[4] Se intenta averiguar una contraseña mediante un enfoque de prueba y error, con la esperanza de acertar.

descifra con la misma clave, como se observa en la siguiente Figura A2. Sin embargo, este método aplica también para acceder a datos en reposo, donde las partes no son directamente personas, sino bases de datos, programas o sistemas de archivos, mediante solicitudes a una interfaz de cliente (KM API), que valida certificados y establece conexiones seguras.

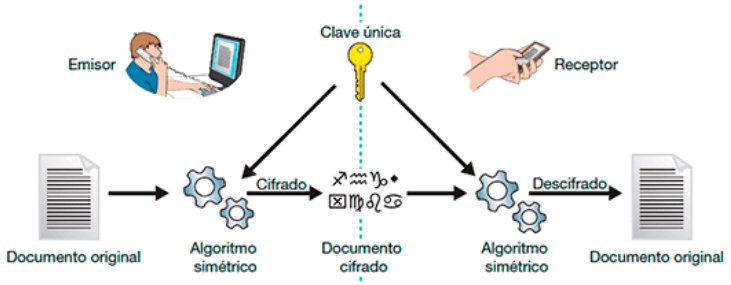


Figura A2. Funcionamiento del software utilizando claves simétricas

Por otra parte, si se utilizan claves asimétricas, las mismas se utilizan para cifrar claves simétricas, que a su vez cifran el archivo (mensaje). La clave pública del destinatario debe ser solicitada por el remitente, de modo que éste último la utilice para cifrar la clave simétrica del documento. Luego, cuando el destinatario recibe el paquete, debe descifrar la clave simétrica utilizando su clave privada. Esta metodología se muestra en la Figura A3:

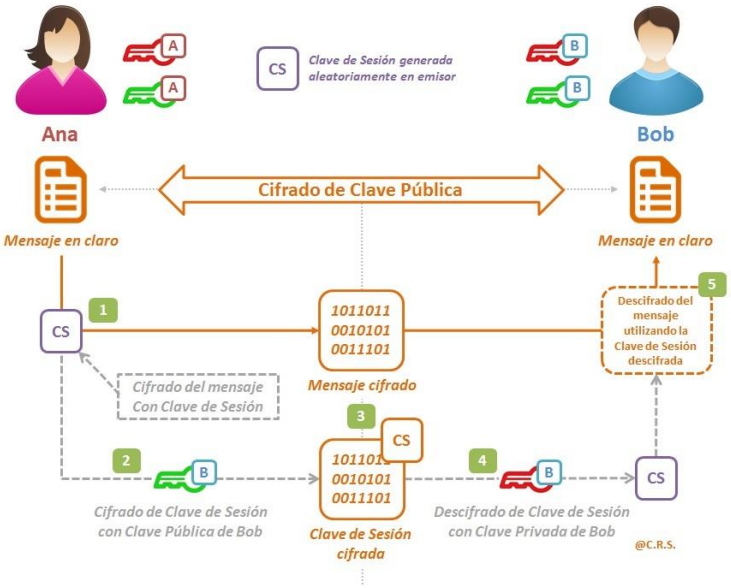


Figura A3. Funcionamiento del software utilizando claves asimétricas

En un sistema distribuido, cada departamento de la organización establece su propio protocolo de gestión de claves, pudiendo haber o no coordinación entre los departamentos.

Apéndice B

Realización de las capacitaciones

A medida que avance el cronograma, se desarrollarán las distintas actividades. Las charlas y capacitaciones consisten en presentaciones con información actual. Donde se usará una habitación de la empresa donde caben todos los empleados, y un proyector para las diapositivas. El orador será un experto en ciberseguridad, el mismo estará disponible para cualquier tipo de consulta durante el periodo que se trabaje. Dramatización en Fig. B1

Figura B1. Dramatización de una capacitación.

La intención es que esta etapa sea dinámica y poco engorrosa para los empleados. Que entiendan la importancia de aprender y comprender los temas. Y asuman su rol como personal.