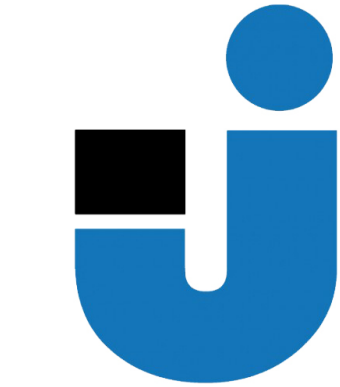

Universidad Nacional
ARTURO JAURETCHE

Seguridad de la Informacióna

TP nº 1

Salvatori Emiliano

Mayo del 2020

Índice

1. Introducción

En el siguiente informe se definen las modificaciones realizadas para la materia **Seguridad de la información Comisión nº 1** a las políticas, normas y procedimientos de seguridad informática según el escenario planteado para la empresa ABM

2. Objetivos

La implementación realizada para este trabajo se basa en los siguientes puntos:

- Conocer el propósito de las políticas, normas y procedimientos de seguridad informática.
- Conocer las principales normas y procedimientos.
- Definir un modelo de normas y procedimientos de acuerdo a un

3. Escenario

La empresa ABC tiene su sede en Capital Federal, posee alrededor de 400 empleados y cuenta con 10 sucursales ubicadas en diferentes ciudades del interior del país, con una totalidad de 20 empleados en cada una de estas sucursales. Para el desarrollo de sus operaciones ABC utiliza un sistema informático desarrollado a medida, el cual comprende un servidor de base de datos sobre el que reside el motor del sistema y un servidor de aplicaciones, también cuenta con un servidor de correo electrónico y un servidor Web para el uso de la Intranet de la empresa. Estos recursos son utilizados tanto por los usuarios de casa central como de las sucursales, siendo Internet el canal de comunicaciones empleado por estas últimas a través de accesos banda ancha. La sede central de ABC posee un acceso a Internet de 2 Mbps protegido por un firewall Cisco PIX 515 con tres interfaces LAN.

4. Modificaciones a los grupos

4.1. Tratamiento de la información

Para establecer un correcto uso de la información, se debe contar con una clara jerarquía de las capas que hará uso de ella, identificando de esta manera cada nivel de seguridad dependiendo a qué cargo se pertenezca. Para ello se debe identificar también cada empleado con dicha estratificación, estableciéndole el nivel de seguridad asignado a la capa que le concierne.

Se deben diseñar para cada nivel los protocolos de acceso, las obligaciones y sanciones que se conllevan en caso de infringir los preceptos establecidos. Se debe identificar el personal encargado de hacer valer y custodiar que estas normas sean llevadas a cabo, tanto hacia adentro de la entidad como también hacia afuera, velando que ningún dato o información sea difundida por fuera del nivel establecido.

Asimismo, se debe contar con herramientas que aseguren la transferencia de datos e información de forma segura entre el personal autorizado, asegurando que esta transferencia se haga de forma encriptada de punto a punto.

Una vez establecido el flujo por el que se transmitirá la información desde abajo hacia arriba y viceversa, la siguiente obligación será la de mantener copias de seguridad de forma diaria, estableciendo a futuro la mejor manera de resguardar este activo, ya sea de forma interna (en equipos provistos dentro de la entidad) o de forma externa (en empresas que brinden el servicio de almacenaje a terceros). En cualquiera de ambos casos, se debe contar con procedimientos que expliciten de forma clara y concisa cómo se debe recuperar la información perdida en caso de alguna contingencia.

4.2. Administración de Usuarios

Como se hizo mención en la sección anterior, se debe establecer la jerarquía de capas por las que la información deba de transcurrir. Una vez realizado este primer punto, se deben utilizar políticas específicas para cada grupo perteneciente a cada nivel o estrato empresarial.

Se deberá contar con contraseñas seguras para toda la grilla de empleados, monitoreando el nivel de seguridad de las contraseñas, debiendo estar establecidas a una longitud mínima de ocho caracteres, incluyendo números, mayúsculas y minúsculas y caracteres especiales. Se debe definir también el cambio de contraseña cada 30 (treinta) días, no pudiendo repetir las contraseñas ya utilizadas en períodos anteriores.

El área encargada de monitorear los usuarios, deberá contar con privilegios de superusuario para poder recuperar claves, usuarios o información inaccesible por alguna contingencia que haya ocurrido con el empleado.

4.3. Ambiente de procesamiento

Como se hizo mención en la sección nº 4.1 (Tratamiento de la información), se requerirá que toda la información se encuentre encriptada de punto a punto. La misma será transferida teniendo en cuenta la jerarquía impuesta para su uso, confiando en no transgredir los niveles de información sensible hacia estratos menos significativos o más bajos.

El uso de los canales y sistemas de comunicación estará estrictamente restringido a los asuntos que conciernen o atañen a la empresa.

Las conexiones deben estar filtradas por un Firewall con políticas restrictivas. Asimismo, se debe establecer una VPN para el uso de la intranet entre sucursales y también para usuarios que no se encuentren dentro de los establecimientos de la empresa ABC.

Se deberá monitorear de forma permanente el tráfico de la red de la entidad, tanto en la red periférica como en la red interna o central; estableciendo procedimientos para este intercambio de la información.

Cuando su uso lo requiera, se brindarán canales especiales para aquella información que sea considerada como sensible para una mayor seguridad sobre la red, disminuyendo cualquier riesgo de ataques tanto directos como indirectos sobre tal activo.

4.4. Correo electrónico y uso de Internet

Los lineamientos deben seguir lo establecido en el punto nº 4.3 (Ambiente de procesamiento), donde se establece que los canales y la comunicación en general estará estrictamente restringida a los asuntos de la empresa. También, se debe dar cuenta de las precauciones que se deben tener en mente a la hora de abrir los distintos correos electrónicos. Para ingresar a este, se deberá hacer uso del usuario y contraseña constituidos por la empresa ABC.

Cada persona empleada dentro de la empresa, debe ser responsable del contenido y del uso que hace de la información contenida tanto en el correo electrónico como en cualquier medio disponible en Internet para su uso. Este será regulado según la jerarquía de niveles mencionada en la sección nº 4.1.

Los usuarios deberán seguir normas establecidas por parte de la entidad, que establezcan restricciones para las descargas de todo tipo, copias o ejecución de archivos o comprimidos.

La empresa deberá contar con herramientas centralizadas para el resguardo de ataques de tipo malware, virus, o cualquier otra amenaza externa, y deberá de ser proveída a todos los dispositivos que tenga en su haber y que sea destinado a su actividad comercial, es decir, tanto en los servidores como en cada uno de los terminales.

Se debe monitorear las actualizaciones de forma periódica del software utilizado para los fines de la empresa, instando al personal a tener al día los terminales de uso comercial.

Se deberá de llevar acabo con todo el personal de la empresa, cursos presenciales o en línea, cuya finalidad sea capacitarlos regularmente para detectar posibles correos maliciosos que no tienen otra finalidad que la de obtener información restringida.

Se deberá contar con un protocolo de seguridad dirigido a bloquear páginas que no cumplan con las normas de seguridad que la empresa vea conveniente, así como páginas que provean posibles canales de ataques a la empresa o a sus empleados.

4.5. Protección física y copias de respaldo

Se requiere que el área dedicada a la administración de sistemas (IT), aplique un control o monitoreo de todas las áreas conformadas por la empresa. Para ello será necesario tener un inventario de todos los equipos, herramientas y los distintos niveles de jerarquía al cual pertenecen, como también tener definidas las herramientas con las que deben contar para llevar a cabo el trabajo diario.

Establecer grupos de soporte eléctrico en caso de que suceda alguna contingencia que deje sin efectos la red eléctrica de uso diario; junto con ello se establece un cronograma para realizar las copias de respaldo de toda la información que se precie de ser indispensable. La información de respaldo en este caso debe contar como se dijo en la sección nº 4.1 con un programa de resguardo y recuperación que especifique la forma que se debe restablecer la información en caso de que suceda alguna contingencia como la suspensión del servicio eléctrico.

Se deben efectuar diariamente copias de seguridad, realizando pruebas periódicas para testear el correcto recupero de la información que sea propensa a ser sustancial, para el desarrollo de la actividad comercial.

5. Continuidad de Procesamiento y Licencias de Software

Es requisito definir los riesgos ante una contingencia sobre el procesamiento de la información. Para ello será necesario establecer previamente el tiempo máximo con el que se pueda disponer de esta sin que impacte de forma significativa en el desarrollo de la actividad comercial de la empresa.

Cada software instalado en las terminales y dispositivos destinados a la actividad de la empresa debe estar bajo su nombre, y contar con una licencia legal para su utilización en el desarrollo comercial. Esta actividad de instalación debe ser monitoreada constantemente para prohibir el uso de software propietario que no esté bajo el amparo legal de la compañía. En caso de que los programas sean con licencias del tipo GPL, se deberá de evaluar con el equipo técnico competente para ver los alcances comerciales que dicho software puede proporcionar.

Se debe contar con procedimientos para mantener actualizado todos los equipos en sus últimas versiones. El área de Tecnología se encargará de las actualizaciones de software que se relacionen con la seguridad, como también la respectiva a redes.

Ningún usuario al que se le haya destinado un equipo o dispositivo para la actividad de la empresa, podrá instalar ningún software sin la previa autorización del personal del área de Sistemas (IT).

Asimismo, todo software deberá contar con guías, manuales o cualquier documento que provea al usuario del programa, una ayuda para superar cualquier eventualidad que pudiese surgir en el uso cotidiano.

Toda actividad que esté amparada por la utilización de este software deberá de estar documentada y estar disponible para aquellos empleados que requieran hacer uso de las mismas.

6. Conclusiones

Establecer políticas de seguridad es de suma importancia en todo tipo de organización, ya sea privada o pública. Estas políticas deben involucrar a toda persona que sea empleada, ya sea de forma eventual o trabaje de forma indefinida en la empresa. Estas políticas deben ser conocidos por todos los empleados y estar disponible al alcance de todos ellos, para su eventual comprensión y modificación en caso de que sea necesario. Estas políticas aseguran la disponibilidad, integridad y confidencialidad de la información de toda la organización.

7. Herramientas

7.1. Materiales utilizados para el presente trabajo

Para la resolución del presente Laboratorio se utilizaron las siguientes herramientas:

1. Arch Linux V5.1.11

2. Para la composición del presente Informe se utilizó el paquete *texlive-latexextra 2018.50031-1*