Universidad Nacional de Tucumán
Facultad de Ciencias Económicas
Asignatura: “Seguridad y Control en Sistemas Informáticos”

DIAGNOSTICO DE MADUREZ DE LA SEGURIDAD DE LA INFORMACION EN EL COMERCIO ELECTRONICO DE UNA PYME TUCUMANA

DIAZ GUZMAN, MATIAS
LORENZO, CAMILA
PFISTER PETERSEN, JERONIMO
ROJAS WDOVIAK, ALEJO
ROMERO, MILENA CAROLINA

Año 2022

Por medio de la presente, los autores manifiestan conocer y aceptar el “Reglamento para la Presentación de Trabajo Final” vigente de la asignatura “Seguridad y Control en Sistemas Informáticos”, haciéndose responsables por la totalidad de los contenidos del presente documento, los cuales son originales y de creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación nacional e internacional de Propiedad Intelectual.

DIAZ GUZMAN, MATIAS
LORENZO, CAMILA
PFISTER PETERSEN, JERONIMO
ROJAS WDOVIAK, ALEJO
ROMERO, MILENA CAROLINA

FIRMADO

1 INDICE

2 INTRODUCCIÓN DE LA EMPRESA 3
2.1 CIBERAMENAZAS (MARCO TEORICO) 4
3 TIPOS DE ATAQUES QUE SUFRE "RODADOS SRL" 5
4 NIVEL DE MADUREZ 6
4.1 ACTUAL 6
4.2 ESPERADO 6
5 ANÁLISIS DE RIESGO: PROBABILIDAD X IMPACTO 7
6 PUNTOS CRITICOS DE SEGURIDAD 7
7 PLAN DE SEGURIDAD 8
7.1 A CORTO PLAZO (6 A 9 MESES) 8
7.2 A MEDIANO PLAZO (9 A 18 MESES) 8
7.3 A LARGO PLAZO (18 MESES A 3 AÑOS) 9
8 ASPECTOS A DESTACAR EN LA EMPRESA 9
9 FUENTES: 11

2 INTRODUCCIÓN DE LA EMPRESA

La empresa que analizamos es anónima, pero para referirnos a ella utilizaremos el nombre de “Rodados Pyme”.
Rodados Pyme es una bicicletería, cuya actividad es el comercio de bicicletas, componentes e indumentaria. Surgió a partir de la idea apasionada de dos amigos ciclistas en un contexto de pandemia en el año 2020, con el objetivo de integrar a más personas a la comunidad del ciclismo.
La visión, la misión y los valores de la empresa fueron desarrollados por los socios de manera informal, ya que todavía se encuentran desarrollandola.
La **visión** de la Pyme es ser la líder en la industria de la bicicleta, atrayendo a personas apasionadas de este deporte, ser proactivos en cuanto al cuidado medio ambiente, contribuir a una vida saludable y proveer medios de transportes sustentables.
La **misión** es ofrecer al cliente un servicio rápido y de fácil acceso para que los aficionados y profesionales del ciclismo puedan salir a pedalear con un equipo de calidad.
Los **valores** son el compromiso con el cuidado del medio ambiente, el trabajo en equipo y la diversidad de personas.
Iniciaron con la propuesta de una página web de fácil acceso y luego abrieron un local comercial físico con venta presencial al público. La principal fuente de ingresos proviene del comercio electrónico, es decir sus actividades operacionales están enfocadas fuertemente en este medio de venta.

Dado el contexto global del año 2020, en donde la venta presencial se vio afectada, las personas buscaron otro medio para poder hacer compras sin necesidad de movilizarse de sus casas y que el producto llegue a su casa. Es importante mencionar también, que el ciclismo era uno de los pocos deportes permitidos bajo normas legales. Es así, que esta situación impulsó a la empresa para el logro de sus objetivos que se vieron cumplidos satisfactoriamente logrando resultados exitosos.

Durante sus inicios la página web fue creada por uno de sus socios. En ese entonces, el diseño y la seguridad de la conexión fueron desarrolladas con un conocimiento básico. Luego, se contrató a personal capacitado en el tema, y es así que logró incrementar el alcance en los clientes y las ventas.
En este entorno de globalización, las leyes que rigen al comercio quedan un poco obsoletas para este medio, y es aquí donde entra lo que denominamos ciberseguridad de la información. La ciberseguridad es un elemento clave para esta gran red de transacciones económicas multitudinarias y proteger los activos informáticos (datos de usuarios, claves, información confidencial de la organización, etc.) se vuelve fundamental en este modelo de negocio.
Siguiendo la historia de *Creeper y Reaper* (1971), donde el primer virus y el primer antivirus surgieron, creemos que no podemos lanzar una página web o en este caso, una página de transacciones económicas totalmente vulnerable sin ningún tipo de protección ante las amenazas ya existentes en el mundo.

RESUMEN
Nuestro trabajo es el análisis de madurez sobre la ciberseguridad del comercio electrónico de una pequeña pyme. En él, destacamos la importancia de la ciberseguridad en el comercio electrónico, las posibles amenazas tanto hacia el sistema como hacia las personas, realizamos un análisis de riesgo sobre las vulnerabilidades que posee, y finalmente un plan de seguridad a seguir a través del tiempo junto con los objetivos divididos por plazos, para evitar futuras perdidas tanto económicas como de confianza de los clientes y de cualquier índole.
Palabras clave: ciberseguridad, comercio electrónico, plan de seguridad.

PLANIFICACION DE LA INTERVENCION Y SU SEGUIMIENTO

Se destacan como objetivos principales de este trabajo de investigación el análisis y diagnóstico de la madurez empresarial actual en materia de ciberseguridad y el diseño e implementación de políticas y estrategias para el fortalecimiento de la seguridad informática de la empresa en su segmento de comercio electrónico (venta y servicios posventa llevados a cabo en su página web).

Nos vinculamos con la empresa, porque una de nuestras integrantes forma parte del equipo de la administración del comercio electrónico y es por ello que pudimos tener acceso a una entrevista con los dueños de la organización.

El trabajo se desarrolló en un ámbito de colaboración y contacto continuo con la empresa, atendiendo las necesidades más urgentes de la organización y desarrollando ideas alineadas a su estrategia y objetivos empresariales, mediante la comunicación y buena predisposición de sus socios con nuestro grupo.

Para estudiar y diagnosticar la madurez de la organización se realizaron análisis de riesgos basándonos en las distintas vulnerabilidades detectadas, lo cual permitió obtener información acerca del estado actual de la organización y comenzar a desarrollar las políticas y planes, basándonos en controles claves y en el desarrollo de métricas apropiadas, que se deberán aplicar para lograr la robustez y seguridad deseada en la empresa.

2.1 CIBERAMENAZAS (MARCO TEORICO)

Los ciberdelincuentes tienen principalmente dos formas de atacar al comercio virtual y a la información que éste contiene:

- Podrán acceder por medio de las personas que trabajan en la empresa (con ataques de *phishing* o trabajos de ingeniería social)
- Mediante vulnerabilidades propias del sistema de la tienda virtual (Malware, Inyección SQL, etc.).

Un **activo de información** se puede definir como cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Pueden ser: procesos de negocio datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización (INCIBE)

Tipos de ataques contra sistemas y contra las personas

Fuente: Presentaciones de clases de la materia Seguridad y Control en Sistemas Informáticos

El principal desafío para las organizaciones es detectar sus principales vulnerabilidades y el impacto que tendrían en la empresa en caso de ser explotadas por ciberdelincuentes.

Luego de realizar un apropiado inventario de activos de información y de desarrollar minuciosos análisis de riesgos a dichos activos y estableciendo umbrales de riesgos las organizaciones deben tomar la decisión de transferir, mitigar o aceptar los distintos tipos de riesgos a los cuales se encuentra expuesta.

3 TIPOS DE ATAQUES QUE SUFRE “RODADOS SRL”

Al consultar con directivos de Rodados S.R.L expresaron, en base a sus experiencias, que las principales amenazas a las que se encuentra expuesta la empresa son las que atentan contra colaboradores y empleados de la empresa como ser:

Ingeniería social: Consiste en persuadir y engañar a una persona para intentar conseguir datos e información sensible. La ingeniería social es uno de los vectores de ataque más peligrosos y que más se está utilizando para acceder a las redes de las organizaciones, haciendo uso de los empleados de las propias organizaciones para vulnerar sus medidas de defensa.

Envío urgente: En este tipo de fraude un supuesto “cliente” manifiesta con mucho énfasis la necesidad urgente de adquirir el articulo (por ser el regalo para un cumpleaños por ejemplo), acto seguido envía un comprobante de transferencia bancaria falsificado para que luego el comerciante prepare y despache el pedido rápidamente para cumplir con el pedido.

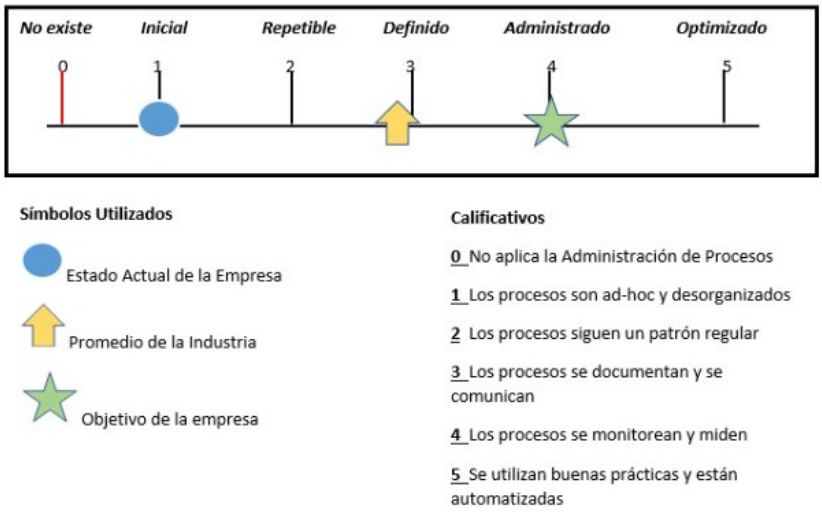
Phishing: El *Phishing* dirigido a empleados de la empresa se ha convertido en el intento de ataque más frecuente sufrido por la organización. Consiste en la recepción de mails con contenido malicioso (archivos adjuntos con *malware*, links a páginas falsas, etc) enviados por ciberdelincuentes con el fin de conseguir contraseñas, instalar *malware* en los sistemas de la empresa o robar datos sensibles de la empresa.
Fraude Amigo: En este caso la compra y el pago son legítimos por parte del cliente, sin embargo, cuando se despacha y recibe el pedido, el cliente desconoce esta compra con su entidad bancaria, perjudicando a la empresa ya que no recibirá el dinero por la compra y tampoco podrá recuperar su mercancía.

4 NIVEL DE MADUREZ

4.1 ACTUAL

La organización se encuentra en un nivel de madurez inicial (1), es inmadura, de acuerdo con el modelo de nivel de madurez.

Modelo de madurez de ciberseguridad en las empresas



Fuente: Edición propia.

No hay una evaluación de riesgos, vulnerabilidades, ni gestión ni documentación de la misma, lo que podría generar en el futuro grandes pérdidas económicas y físicas de los activos informáticos.

4.2 ESPERADO

A través del plan de seguridad que implementaremos, se espera que la organización este en el nivel de madurez número 4 en el que los procesos se monitorean y miden con las métricas que se establecerán.
Se espera que el comercio electrónico sea un medio seguro tanto para la persona que intenta realizar una transacción, como para la organización, resguardando los datos de los usuarios que ingresan y resguardando los movimientos que en ella se hacen.
Además, también se espera que paulatinamente los empleados estén lo suficientemente capacitados y adquieran una cultura de conciencia en ciberseguridad para no brindar datos de tipo confidencial y preservar la integridad de los mismos.

Se busca por último, que la experiencia dentro del sitio web sea la más segura y cómoda para los clientes de la organización.

5 ANÁLISIS DE RIESGO: PROBABILIDAD X IMPACTO

Matriz de Riesgo

Fuente: Presentaciones Power Point de clases.

El riesgo de la organización es muy alto, ya que la probabilidad de ocurrencia de un evento por falta de seguridad es alto, y el impacto que esté tendría, es alto igualmente.

6 PUNTOS CRITICOS DE SEGURIDAD

En lo que respecta a “Rodados Pyme” el principal vector de ataque al que está expuesta la empresa es hacia las personas. Hasta ahora, no sufrieron ningún tipo de ataque contra el sistema pero de sufrirlo, no cuentan con un plan de recuperación o un procedimiento a seguir.

- No cuentan con un encargado de la seguridad de la información, ni tampoco un Comité de Seguridad.
- Ausencia de un plan de capacitación en cuanto a ciberseguridad para los empleados y directivos.
- Los activos de información, no están individualizados ni inventariados;
- Existe una gran dependencia de conocimientos externos ante incidentes de ciberseguridad.
- No hay políticas ni procedimientos documentados establecidos para la gestión de la seguridad.
- No existen políticas ni protocolos a seguir en cuanto al almacenamiento seguro y protección de datos personales de clientes
- Detección de compras fraudulentas: Existe un protocolo en al momento de que el cliente realice una compra, pero no tienen claro que destino y medidas de seguridad se aplicarán a los datos que se recaban en esta etapa (Foto de DNI, Foto del cliente con medio de pago y DNI)

7 PLAN DE SEGURIDAD

Un plan de seguridad ayuda a disminuir las vulnerabilidades e incrementar las capacidades para dar respuesta a las amenazas o reducir la probabilidad de ocurrencia, reduciendo así el riesgo.
Es preferible tener un plan de seguridad sencillo para que los miembros de la organización implementen, en vez de un plan complejo que seguramente no implementarán.
Por ello recomendamos el siguiente plan:

7.1 A CORTO PLAZO (6 A 9 MESES)

Objetivo: Conformar bases sólidas en materia de ciberseguridad para la mejora de la empresa
:

- Definir al o los responsables de la información;
- Realizar inventario de los activos de la información
- Determinar las competencias que debe tener cada miembro de la organización para el manejo de los activos de información.
- Seguridad en el formulario de carga de datos por parte de los clientes, a fin de evitar que se puedan obtener los datos que se carguen en ellos.
- Seguridad y mantenimiento de los servidores.
- Plan de capacitación y concientización a los empleados y directivos, para manejo de los datos de los clientes (datos personales, usuarios y medios de pago).

7.2 A MEDIANO PLAZO (9 A 18 MESES)

Definir las políticas de Control y Cumplimiento de los objetivos en Seguridad que se irán definiendo a medida que se avance en la implementación de Seguridad.

- Crear e implementar un Plan de Continuidad del Negocio (BCP);
- Firewalls y niveles de acceso a la base de datos de la empresa que permitan el resguardo de los datos de los clientes, evitando los ataques tanto externos como internos;
- Autenticación en dos pasos al momento de realizar los pagos a través de la plataforma web de comercio electrónico, ya sea tanto incluyendo los datos de los medios de pago como de la persona que compra;
- Destinar una partida del presupuesto de la empresa a Inversiones en Seguridad de la información y a los activos de información que posee o se adquieran.
- Elaboración de un plan de tratamiento del riesgo.

- Creación de un comité de seguridad de la información;

- Analizar la factibilidad de implementar controles CIS:

Con esto pretendemos mejorar parte de la seguridad que ya tiene implementada la organización. Incluyendo un proceso de evaluación constante a fin de ir mejorando este plan.

7.3 A LARGO PLAZO (18 MESES A 3 AÑOS)

Una vez establecidas y comunicadas las bases de la ciberseguridad y que las políticas guían el curso de acción de toda la organización, es necesario clasificar los posibles riesgos que pueden surgir eventualmente para establecer medidas de protección adicionales así como también crear estándares de monitoreo y administración para verificar que el avance de nuestro plan estratégico se adecua con esos estándares o hay que implementar medidas correctivas.

-Auditorías internas y externas de ciberseguridad: Se deben establecer pruebas con regularidad como el Test de Penetración, para verificar el cumplimiento de las pautas de seguridad y comprobar que tan bien están funcionando las medidas de protección ante ataques.

-Actualizar *hardwares* obsoletos para la continuidad de las tareas habituales de forma rápida y eficiente. Además, se podrá contratar servicios antimalware más fuertes en dispositivos más actualizados.

-Definir, implementar métricas para la efectividad del programa de ciberseguridad: el presupuesto utilizado y el impacto costo-beneficio que tuvo, comparar con otras organizaciones el nivel en el que estamos, el nivel de riesgo en el que nos encontramos y cuanto de ese riesgo pudimos minimizar.

-Establecer medidas correctivas en caso de que hubiera, para mejorar el plan de seguridad.

-Indicar el grado de cumplimiento de los objetivos de seguridad establecidos en el corto y mediano plazo.

8 ASPECTOS A DESTACAR EN LA EMPRESA

Si bien la empresa no es un ejemplo de las buenas prácticas de seguridad, debe destacarse que si poseen interés en realizar mejoras en la seguridad y tienen la predisposición para realizarlo.

Encontramos ciertas prácticas que si bien no son idóneas demuestran un interés en materia de seguridad por parte de la empresa como ser:

1. Cuentan con un equipo de trabajo reducido, por lo que introducir un plan de capacitación y un cambio de cultura radical dentro de la empresa resulta mucho más fácil y rápido que en una empresa de gran envergadura.
2. Existe una muy buena predisposición de la organización para mejorar respecto a su nivel de madurez en el comercio electrónico.
3. En los servidores críticos el *backup* es diario, y los equipos no críticos tienen un respaldo.
4. Se solicita por mail la baja de un usuario. RRHH informa por mail la baja del personal y solicita la quita de los accesos a las páginas web.
5. Cuentan con un protocolo a seguir para identificar a la persona que adquiere una compra a través del comercio electrónico.

RESULTADOS

Como principales resultados logramos en primer lugar obtener un diagnostico sólido del estado actual de la organización en lo que respecta a la ciberseguridad de sus activos informáticos, el cual lo calificamos de inmaduro y en una escala de madurez desarrollada la ubicamos en un nivel inicial de madurez.

Otro resultado obtenido es el desarrollo de políticas y buenas prácticas de seguridad informática, alineadas a la estrategia empresarial, destinadas a mitigar los riesgos vinculados a las principales vulnerabilidades detectadas en la organización.

CONCLUSIONES

En base a la información recolectada y el análisis realizado en el trabajo, creemos que brinda un beneficio y guía para la toma de decisiones de la organización a la cual entrevistamos. Permitiendo que la misma tome más conciencia sobre las vulnerabilidades que posee y las pérdidas que podría generarse en el futuro en caso de no tenerlas en cuenta.

Por otro lado, nos gustaría destacar la dificultad para obtener la información confidencial de la empresa como la principal limitación de nuestro trabajo. En cuanto a las líneas futuras creemos que el emprendimiento podría destacar el área de ciberseguridad del comercio electrónico debido a que es el canal de ventas que sostiene actualmente a la organización y presenta la mejor proyección a futuro.

9 FUENTES:

Fuente 1: Nos contactamos con uno de los dueños de la empresa para hacerle la siguiente entrevista y fue esta herramienta la que utilizamos como base para el trabajo:

El comercio electrónico está funcionando muy bien, va de manera escalonada en nuestra tienda, nosotros aprendiendo a cómo manejarlo cada vez más, puliendo detalles y hay que ser muy ordenados en el manejo de la tienda virtual, la manera de llegar hacia el cliente brindando la confianza que necesita, siendo prolijos y claros para no marearlo.
Cada vez más gente está recurriendo a las tiendas virtuales, ya sea por comodidad o falta de tiempo basándose en el comercio rápido, comprando desde cualquier lado y que llegue en un tiempo muy rápido, por algo Mercado Libre o Pedidos Ya están entre las empresas con mayor crecimiento en los últimos años en el país, y son las que siguen creciendo sin techo.

¿Qué medidas de seguridad tiene? ¿Poseen algún plan de recuperación ante algún ataque?

En cuanto a la web, contamos con un *backup* automático de toda la información de los productos, fotos, características, precios para resguardarnos ante cualquier situación que pueda pasar, aunque no creo que sea tan sencillo como suena.

¿Alguna vez sufrió algún ataque a las personas o al sistema?

No sufrimos ningún ataque al sistema en sí, es decir a la plataforma, pero si sufrimos constantemente ataques mediante los intentos de fraude, ya sea realizando compras con tarjetas y documentación robada o tarjetas clonadas.

¿Toman algún tipo de precaución o cuentan con un protocolo a seguir ante ataques a las personas?

Por suerte las primeras veces, evitamos entregar bicicletas, cuando el camión ya estaba en repartición, sin saber que esto podía suceder tan fácil.
Desde ese momento nos informamos y pedimos una serie de datos para verificar la identidad, y una vez validados los datos procedemos al proceso de venta del producto (esto lo hacemos con montos superiores a $50.000, sino sería muy engorroso validar todas las compras)

¿En qué consiste este procedimiento?

Proceso de validación para venta online o Whatsapp con tarjeta.

1- Enviar foto del DNI de frente y dorso
2- Enviar foto del rostro de la persona con el DNI al lado
3- Enviar foto del frente de la tarjeta (tapando los números, menos los últimos 4), no enviar foto del dorso de tarjeta para no saber el código de seguridad
Una vez que se cumplan estos requisitos, pasaremos al proceso de validación, para poder generar el link de pago.

¿Cómo funciona el comercio electrónico?

El proceso completo para que el comercio electrónico funcione está administrado por 6 personas

Una persona y un asistente (de refuerzo) encargada de subir el contenido (fotos y características) y encargada de modificar las secciones de novedades, ofertas, fotos de la página. Además de que es la encargada de poner los precios a los productos y controlar que estén actualizados constantemente

Una persona encargada de controlar el stock y codificar todos los productos para poder tener lo más ordenada posible la tienda online (este puesto es reciente y está teniendo éxito en cuanto al orden de la tienda online)

Una persona en línea con celular y pc encargada de contestar las consultas y dudas para terminar de realizar las compras en muchos casos, y encargada de pedir los datos para verificación de identidad

Dos personas encargadas de armado de pedidos.

¿Hay concientización sobre los ataques tanto dentro de la organización como para los clientes?

Si totalmente y es por eso que tenemos el proceso de validación de compras.

Y el proceso de compra se gestiona mediante mercado pago, plataforma de pago costosa, pero brinda la seguridad de compra para el usuario.

Fuente 2:

- Gestión de riesgos (INCIBE): Una guía de aproximación para el empresario
- ISO 31.000
- Ciberamenazas contra entornos empresariales (INCIBE)
- Ciberseguridad en comercio electrónico (INCIBE)
- Copias de seguridad (INCIBE)