EVALUACIÓN Y PROPUESTA DE MEJORA DEL NIVEL DE MADUREZ DE SI EN UNA EMPRESA COMERCIAL

Seguridad y Control de Sistemas Informáticos Cohorte 2024

Dall'Agata Ornella- Oyanguren Tapia Carlos Gabriel-

Plaza Valentina- Vazquez Benjamin

ornelladallagata@gmail.com - gabrieloyan2001@gmail.com -

valentinaplaza02@gmail.com - benjaminv1010@gmail.com

Resumen

El presente análisis tiene como objetivo evaluar el nivel de madurez en seguridad de la información de la empresa XX, líder en la comercialización de tecnología y servicios técnicos. Para ello, se utilizó una encuesta basada en una escala de Likert modificada, aplicada a la jefa del sector de ventas, encargada del sistema de gestión. Los resultados obtenidos, analizados mediante el modelo de madurez de Gartner, indicaron que la empresa se encuentra en el Nivel 1 (Inicial), con una implementación mínima de prácticas de seguridad y la ausencia de políticas formales. Se identificaron áreas críticas de mejora, como la falta de roles y responsabilidades definidas, políticas de seguridad documentadas y programas de capacitación.

Las recomendaciones incluyen formalizar políticas de seguridad, establecer roles claros, implementar autenticación multifactor, desarrollar procesos de gestión de accesos y crear un programa de concientización. Se espera que, con la implementación de estas acciones, la

empresa alcance el Nivel 3 (Definido) en seguridad de la información en un plazo de 12 a 18 meses. Esto fortalecerá la protección de la información y mejorará la confianza de los clientes, apoyando su crecimiento y expansión.

Palabras clave: Madurez de seguridad, política de seguridad, concientización.

Tabla de contenidos

Introducción a la empresa

La empresa que analizaremos es anónima, para referirnos a ella utilizaremos el nombre XX. Situando su sede central en San Miguel de Tucumán y con varias sucursales en Tucumán, XX se ha consolidado como una empresa líder en la comercialización de tecnología como por ejemplo celulares, electrodomésticos, consolas, etc. También ofrece servicio técnico para todos estos productos y cuenta con una amplia gama de accesorios (fundas, cargadores, templados, etc).. Con un enfoque centrado en la calidad y la atención al cliente, la empresa ha logrado construir una sólida reputación en el mercado local. Desde su inicio, ha experimentado un crecimiento constante, ajustándose a las demandas de un público cada vez más exigente y tecnológicamente informado. Esto le ha permitido atraer a una amplia variedad de clientes en busca tanto de productos de uso diario como de soluciones tecnológicas avanzadas.

Misión: La misión de XX es proporcionar a sus clientes productos de alta calidad, accesibles y que mejoren la calidad de vida en el hogar. Además, ofrecen un servicio técnico confiable para garantizar la durabilidad y el funcionamiento óptimo de los productos. Su enfoque es brindar soluciones tecnológicas que faciliten las tareas diarias y respondan a las necesidades cambiantes de sus clientes.

Visión: Ser la empresa líder en Tucumán en la venta de productos y servicio técnico, destacándose por su atención al cliente, servicio postventa y la calidad de ambas. Aspiran a ser reconocidos por su compromiso con la satisfacción del cliente, con planes de expansión hacia nuevas áreas del norte del país, aprovechando las oportunidades tecnológicas para mejorar el acceso y la experiencia de compra.

XX opera en un entorno competitivo dentro de la provincia de Tucumán, donde el mercado de tecnología está en expansión. Las demandas de los consumidores por tecnología eficiente, moderna y sostenible están en constante aumento. La tienda se enfrenta a la competencia tanto de grandes cadenas nacionales como de tiendas locales, pero se diferencia por su enfoque en el servicio técnico post venta de varios productos, que brinda una ventaja competitiva al ofrecer soluciones rápidas y efectivas.

La empresa para el manejo tanto de la casa central como sus sucursales, utiliza dos sistemas de gestión: *InfoManager* y *Gestioo*, ambos centralizados. *InfoManager* es utilizado en los circuitos de compra, venta, facturación y movimientos de stock. La función de *Gestioo* tiene relevancia en el área y circuito del servicio técnico, en el que se recepcionan los equipos y se hace un seguimiento de las distintas etapas, comenzando desde la recepción, hasta su respectivo control de calidad y puesta a punto para que los equipos sean entregados a los clientes.

Consciente de la importancia de proteger los datos de sus clientes y la integridad de sus sistemas, la empresa ha implementado algunas medidas básicas de seguridad. Sin embargo,

ante un entorno competitivo y las crecientes amenazas en el ámbito de la seguridad, es necesario un análisis exhaustivo que permita identificar su nivel actual de madurez en seguridad de la información, para luego implementar mejoras.

La investigación permitirá identificar las brechas de seguridad y las áreas críticas que requieren mejoras. El objetivo es desarrollar recomendaciones que fortalezcan la postura de seguridad de la empresa, minimicen riesgos y garanticen la protección de información sensible. A través de estos esfuerzos, se busca no solo optimizar la seguridad interna, sino también mejorar la confianza de los clientes y reforzar la reputación de la empresa en un mercado en constante evolución.

Planificación de la intervención

Para llevar a cabo la evaluación de madurez en seguridad de la información en la empresa, se utilizó una encuesta como instrumento de recolección de datos, con el fin de obtener una visión precisa de las prácticas actuales de seguridad de la información en la empresa. La elección de este instrumento se debe a su capacidad para recopilar información directa sobre las prácticas actuales de seguridad, permitiendo una visión detallada y específica de los procedimientos internos. La encuesta, compuesta por 12 preguntas (Véase en Anexo 1), fue respondida utilizando una escala de Likert modificada, sin opción intermedia, eliminando la posibilidad de una respuesta "neutra" para poder expresar un nivel claro respecto de cada aspecto evaluado. Participó en la encuesta la jefa del sector de ventas, quien es la encargada de la administración del sistema. Esto asegura que las respuestas reflejen de manera precisa el estado actual de la seguridad de la información y faciliten la identificación de áreas críticas de mejora.

Para evaluar los datos recopilados, se utilizará el modelo de madurez de seguridad de Gartner. Este modelo es adecuado para la investigación porque permite medir de forma estructurada y progresiva el nivel de desarrollo de las prácticas de seguridad de la información dentro de la empresa. El enfoque de Gartner categoriza la madurez en diferentes niveles, desde

prácticas básicas e informales hasta estructuras avanzadas y optimizadas, proporcionando una visión clara del estado actual de la seguridad y las áreas de mejora.

Análisis de la encuesta

Para realizar un análisis comprensivo de los datos cuantitativos obtenidos por medio de la encuesta, a continuación se muestra un gráfico radial que muestra las respuestas dadas por el personal. Las preguntas de la encuesta fueron evaluadas en una escala de Likert, en donde 1 representa "Totalmente en desacuerdo" y 4 indica "Totalmente de acuerdo". Este gráfico permite visualizar de manera clara y comparativa el estado actual de la organización en diferentes áreas de seguridad de la información, como la existencia de políticas formales, la definición de roles y responsabilidades, las medidas de resguardo de datos confidenciales, y la capacitación en seguridad, entre otros.

Fuente: Elaboración propia

El gráfico refleja que la empresa presenta un nivel bajo de madurez en la mayoría de las áreas clave de seguridad de la información, con varias respuestas concentradas en niveles de "Desacuerdo" o "Totalmente en desacuerdo". Las áreas mejor valoradas incluyen la clasificación de datos y el uso de contraseñas únicas. Sin embargo, se observan importantes oportunidades de mejora en aspectos críticos como la definición de roles y responsabilidades, la existencia de políticas de seguridad documentadas y la capacitación en manejo seguro de información y respuesta ante incidentes. Estos resultados respaldan la necesidad de avanzar hacia un nivel de madurez más desarrollado para fortalecer la postura de seguridad de la empresa.

Determinación del Nivel de Madurez Actual y del Nivel de Madurez Ideal

Determinación del Nivel de Madurez Actual en Seguridad de la Información

Para determinar el nivel de madurez actual en Seguridad de la Información de la empresa, se tomó el modelo de niveles de madurez en Seguridad de la Información establecidos por Gartner. Se asignó un rango de puntaje acumulado a cada nivel, de manera que:

1. Nivel 1 - Inicial: 0 a 10 puntos.
2. Nivel 2 - En desarrollo: 11 a 20 puntos.
3. Nivel 3 - Definido: 21 a 30 puntos.
4. Nivel 4 - Gestionado: 31 a 40 puntos.
5. Nivel 5 - Optimizado: 41 puntos o más.

Luego de esto, se desarrolló una encuesta (Ver Anexo 1) con una serie de preguntas clave para determinar el nivel de madurez de la empresa, para ponderar las respuestas de una manera más precisa, se utilizó una escala de Likert, del 1 al 4 y se asignó un puntaje a cada posible respuesta, de manera que:

1. Totalmente en desacuerdo: 0 puntos (indicando un bajo nivel de implementación o inexistencia del control).

2. En desacuerdo: 1 punto (indica una implementación mínima o informal).

3. De acuerdo: 2 puntos (indica una implementación moderada, aunque posiblemente sin formalización completa).

4. Totalmente de acuerdo: 3 puntos (indica una implementación adecuada, posiblemente con formalización).

A partir de lo anteriormente mencionado, y luego de haber realizado la encuesta correspondiente, se concluyó que la organización se encuentra en el Nivel 1 - Inicial de madurez, habiendo sumado un total de 10 puntos. Este nivel se caracteriza por la falta de formalización y sistematización en los procesos de seguridad. En el caso específico de esta empresa, se observó que no cuenta con políticas de seguridad documentadas, los roles y responsabilidades en seguridad no están bien definidos, y no existen programas de concientización o capacitación que permitan a los empleados comprender y gestionar adecuadamente los riesgos. Aunque dispone de prácticas básicas en algunas áreas, como el uso de contraseñas únicas y la clasificación de datos, su enfoque en seguridad es aún reactivo y dependiente de medidas ad hoc, en lugar de una estrategia de gestión planificada.

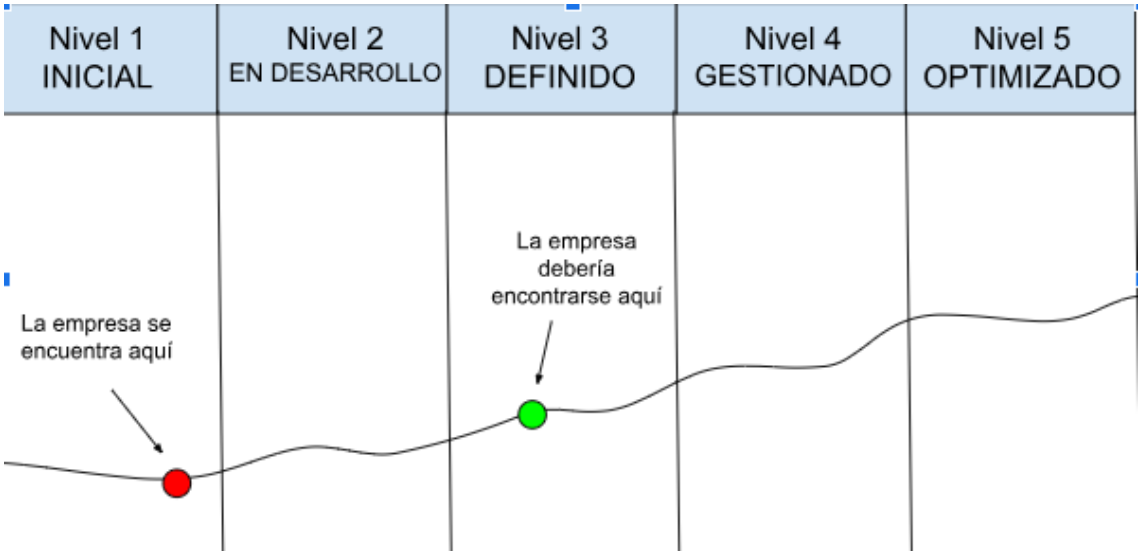
NIVEL DE MADUREZ IDEAL EN SEGURIDAD DE LA INFORMACIÓN

Considerando el contexto en el que opera la organización, su sector comercial y sus objetivos estratégicos, se concluyó que la empresa debería aspirar a alcanzar el Nivel 3 - Definido en el modelo de madurez de seguridad de la información de Gartner. En este nivel, la organización no sólo establecería políticas de seguridad formalizadas, sino que también estructuraría procesos y controles específicos que se implementen de manera consistente en toda la empresa.

Para avanzar hacia este objetivo, se recomienda la adopción de buenas prácticas que incluyan la creación y comunicación de una política de seguridad de la información claramente definida, que sea conocida y comprendida por todos los empleados. Además, es crucial que la empresa formalice los roles y responsabilidades en seguridad, desarrolle un programa de concientización regular para el personal, y establezca procesos documentados tanto para la asignación de accesos a nuevos empleados como para su revocación en caso de cambios de rol o salida de la empresa. Estos puntos se desarrollarán posteriormente.

Al alcanzar el Nivel 3, la empresa mejoraría su capacidad para gestionar y mitigar los riesgos de seguridad de manera proactiva, promoviendo una cultura organizacional más consciente de la importancia de la protección de la información y alineando sus prácticas de seguridad con sus objetivos comerciales.

Todo lo anteriormente mencionado se resume en el siguiente cuadro, basado en los niveles de Seguridad de la Información de GARTNER, tomando como referencia los dos puntos anteriormente desarrollados:



Fuente: Elaboración propia

Resultados

Algunas de nuestras recomendaciones y propuestas para mejorar el nivel de madurez de seguridad de la información de XX son:

1. Formalizar y difundir ampliamente una política de seguridad de la información que sea conocida por todos los empleados. Esta política debe abordar aspectos clave como la clasificación de datos, las responsabilidades de seguridad y las normativas internas. Además, la política debe ser revisada y actualizada periódicamente para adaptarse a las nuevas amenazas y regulaciones.
2. Definir y asignar claramente los roles y responsabilidades en materia de seguridad de la información. Esto incluye la designación de un responsable de la seguridad (como un CISO), así como la creación de un equipo de seguridad que coordine las iniciativas de protección de datos y activos informáticos. Es importante que todos los empleados estén al tanto de sus responsabilidades en relación con la seguridad.
3. Establecer una política rigurosa para crear contraseñas seguras, especificando una longitud mínima y la combinación de caracteres requeridos (mayúsculas, minúsculas, números, y símbolos). Es recomendable utilizar herramientas que verifiquen la fortaleza de las contraseñas y fomentar el uso de autenticación multifactor (MFA) para garantizar un acceso más seguro.
4. Desarrollar y documentar un proceso formal para la gestión de accesos y revocación de los mismos en los sistemas de la empresa. De esta manera, se asegurará que el acceso a los activos de información se otorgue de acuerdo con las responsabilidades y funciones de cada empleado, así como la desactivación inmediata de cuentas de usuario, la recuperación de dispositivos de acceso, y la cancelación de cualquier otro permiso de acceso relevante. Es fundamental que sea eficiente y documentado para reducir el riesgo de accesos no autorizados posteriores a la salida de un empleado.

5. Implementar un programa de concientización sobre seguridad de la información que abarque temas como la protección de datos, prácticas seguras en el uso de dispositivos y la gestión de contraseñas. Este programa debe ser obligatorio para todos los integrantes del área, repetirse de forma periódica y ayudar a desarrollar una cultura de seguridad dentro de la empresa de manera que todos comprendan sus responsabilidades en la protección de la información de la organización.
6. Establecer un procedimiento de respuesta a incidentes que incluya la identificación y reporte de incidentes de seguridad por parte de los empleados. La capacitación debe cubrir la detección de amenazas comunes y el proceso para reportarlas de manera rápida y eficiente a los encargados de seguridad de la información. Este proceso busca preparar a los empleados para gestionar los incidentes y asegurar que se tomen medidas rápidas y eficaces para reducir el impacto de cualquier amenaza a la seguridad de la información

Conclusión

En conclusión, si la empresa implementa las recomendaciones propuestas se espera que en un período de 12 a 18 meses alcance el nivel 3 de madurez en seguridad de la información, según el modelo de Gartner. Este avance permitirá que la empresa cuente con procesos de seguridad formalizados y prácticas consistentes que protegerán eficazmente tanto sus activos como la información de sus clientes.

La adopción de estas medidas contribuirá al cumplimiento de la misión de XX, que se centra en ofrecer productos tecnológicos confiables que mejoren la vida de sus clientes, respaldados por un servicio técnico seguro y de calidad. Al establecer una cultura de seguridad de la información, podrá diferenciarse en un mercado altamente competitivo, destacándose por su compromiso con la protección de la información y la satisfacción del cliente. A su vez, estas

mejoras fortalecerán la confianza en la empresa y consolidarán su reputación, lo cual será clave para apoyar su visión de expansión y liderazgo en el sector tecnológico y de servicios postventa en Tucumán y en otras áreas del país.

Referencias Bibliográficas

- **Center for Internet Security. (s.f.).** *CIS Controls v8.1.* Center for Internet Security. https://www.cisecurity.org/controls/v8-1
- **International Organization for Standardization**. (2022). ISO/IEC 27001:2022 - Information Security Management Systems — Requirements. ISO.
- Gartner. (2023). Maturity Model for Information Security. Gartner Research. https://www.gartner.com
- **Forbes México. (2021, noviembre 2).** *Cómo medir la madurez de ciberseguridad en mi organización.* Forbes México. https://forbes.com.mx/como-medir-la-madurez-de-ciberseguridad-en-mi-organizacion/