TESTEO Y ANÁLISIS DE MADUREZ EN SEGURIDAD DE LA INFORMACIÓN

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

Autores:

- **COLOMAR** Luciano German
- **GARCIA MILLAN** Gonzalo Jose
- **NINA JARMA** Agustina Candela
- **SZABO ARGAÑARAZ** Facundo Jose

Cohorte: 2024
ÍNDOLE DE TRABAJO: Profesional

Declaración jurada del origen de los contenidos

“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”.

COLOMAR Luciano German
GARCIA MILLAN Gonzalo Jose
NINA JARMA Agustina Candela
SZABO ARGAÑARAZ Facundo Jose

1. RESUMEN

El presente trabajo aborda lo que es un diagnóstico en la madurez de la seguridad de la información en un grupo económico, el cual cuenta con seis empresas, de las cuales tienen tres rubros diferentes, en donde tres de estas se dedican a la comercialización, dos están destinadas a la venta de vehículos y una se encuentra en el sector inmobiliario.
En total, este grupo económico cuenta con dieciocho sucursales dentro de la provincia.
El propósito de este trabajo es realizar un análisis del nivel de madurez con el que cuenta la empresa, donde dicha información se va a recolectar mediante una entrevista con personal clave de TI, encargado de la seguridad en los sistemas de información, y realizando además entrevistas a los empleados para contar con mayor información de las diferentes áreas con las que cuenta la empresa.
Una vez obtenidos los resultados sobre la situación actual de la empresa, se realizará un análisis sobre la situación actual en la cual se encuentra Group S.A. destacando sus fortalezas, como así también sus debilidades. Previamente se brindarán recomendaciones para poder eliminar vulnerabilidades que sean explotables, y así podrá mantenerse prevenido y/o preparado para futuras amenazas.

Palabras clave: diagnóstico, madurez de la seguridad, debilidades, amenazas, fortalezas.

TABLA DE CONTENIDOS

1. Introducción……

2. Planificación de la intervención y de su seguimiento……

3. Resultados……

4. Conclusiones……

5. Referencias bibliográficas…….

6. Anexos……

1. INTRODUCCIÓN

En la actualidad, las empresas enfrentan un panorama cada vez más complejo en términos de amenazas cibernéticas, las cuales están en constante crecimiento.
La rápida digitalización de los procesos empresariales, la creciente dependencia de las tecnologías de la información y la expansión de los ataques informáticos han incrementado significativamente los riesgos relacionados con la seguridad de la información.
Por ello, el trabajo de investigación se centra en la evaluación de las prácticas de ciberseguridad implementadas en la empresa, la cual identificamos bajo el nombre de fantasía de “Group S.A.” Está ubicado en la provincia de Tucuman, donde actualmente cuenta con 125 empleados en total.
Group SA cuenta con 35 años de trayectoria en las cuales hasta el momento no presentó ningún ataque de ciberseguridad dentro de la organización.
El objetivo principal de este estudio es identificar las vulnerabilidades existentes en su infraestructura tecnológica, analizar la efectividad de las medidas de protección implementadas y proporcionar recomendaciones para poder mejorar su postura de seguridad frente a las crecientes amenazas cibernéticas.

2. Métodos, planificación de la intervención y de su seguimiento:

La intervención realizada en la empresa consta principalmente de cuatro partes:
-Análisis y conocimiento del grupo económico: para dicha tarea entrevistamos a un empleado administrativo-contable para conocer a grandes rasgos las empresas, su mercado, su personal, dedicación y por sobre todo la visión que tienen a futuro. Con toda esta información queremos obtener un paneo general, conocimiento y rubro el cual estamos abarcando con los parámetros "aceptables" para sociedades similares en el sector.
-Planificación y elaboración del formulario enviado al responsable de seguridad y sistemas de la empresa: esto abarcó la parte más dura y engorrosa del trabajo. Luego de obtener una idea de que empresa estamos tratando adoptamos un enfoque mucho más burocrático, gestacional y de controles debido al nivel de información que maneja el grupo económico dejando un poco de lado la parte más técnica de software o bases de datos aplicadas. Para tal proceso utilizamos como principal guia el "Trabajo practico sobre madurez de la informacion - "Empresa XYZ SA" con enfoque de controles CIS dentro de los cuales los principales temas son: Gobernanza, inventario de seguridad de la informacion, Criticidad de activos, controles de accesos entre los cuales específicamente fisicos, digitales, contraseñas, metodos de autentificacion utilizados, respaldos de infromacion, educación sobre seguridad de la información y concientización, planes ante contingencias. Los resultados obtenidos como la madurez serán profundizados en el anexo "resultados" oportunamente.
Cabe destacar que cada una de las preguntas realizadas con pura y exclusivamente de nuestra autoría con todos los criterios aprendidos a lo largo del cursado tratando de volcarlo a la realidad y de una manera que sean comprensibles para todos ya que consideramos que en la actualidad no todos son conscientes o están involucrados en el tema de la seguridad de la información que nos otorgó dicha materia. (adjuntamos enlace al formulario: " https://forms.gle/Rp6Q9bBMySEhVaK19 "
-Envio de formulario al encargado: el formulario adjuntado arriba fue enviado el dia 24-10-24 al encargado "XX" ya que decidio resguardar su identidad para la realizacion del trabajo y lo respetamos profundamente nos devolvio los resultados el dia martes 5-11-24 adjuntamos las respuestas en el siguiente documento "https://docs.google.com/spreadsheets/d/14bC5OsilettlEgcbyM0RHkyBzMPTSMR_UV9kh303Y5A/edit?usp=sharing" (debe solicitar acceso con el fin de resguardar la información)
-Proceso de información y resultados: una vez obtenida la respuesta decidimos reunirnos para procesarla mediante una escala de:
- Del 1 al 5: correspondiendo 1 para aquellas respuestas que realmente no lo consideran, 2 para aquellas tareas solamente necesarias, 3 un control bueno, 4 Muy bueno y 5 excelente
-A su vez también tenemos respuestas de SI/NO/NO LO CONSIDERAMOS OPORTUNA PARA NUESTRA TAREA: para estas consideramos que todas las respuestas si, son una buena/aceptable madurez de la seguridad en la información; todas las respuestas NO, las observamos en detalle junto a las que NO CONSIDERAN OPORTUNAS, para procesarlas una por una y analizar si realmente está bien que no lo implementen o si es necesario que se tengan en cuenta. Todo esto considerando el nivel de facturación del grupo económico, el

tipo de activo que se está tratando y que tratamiento se le quiere otorgar a los riesgos, es decir: si se los desea transferir, aceptar, mitigar o tratar.

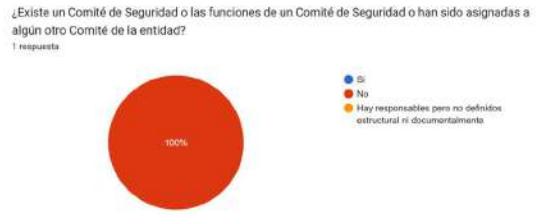
Para determinar el nivel de madurez de seguridad de la informacion nos basaremos en **CONTROLES CIS (aplicado en el "TP EMPRESA XYZ SA") criterios y conocimientos formados a lo largo del cursado.**

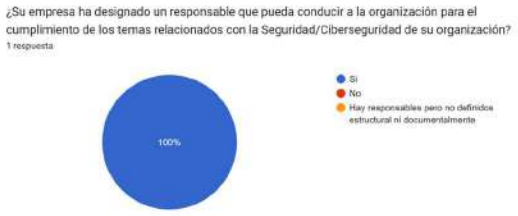
Una vez conocido el grado de madurez de seguridad de la información, se procederá a realizar una serie de sugerencias a la dirección de la empresa para elevar su nivel de seguridad y proteger sus activos de información. El objetivo es poder hacer sugerencias tanto que no requieran una fuerte inversión económica como aquellas que quiza si sea necesario o beneficioso para la organización.

3. RESULTADOS

A través del cuestionario enviado al entrevistado se obtuvieron los siguientes resultados relativos a madurez de la seguridad de la información:

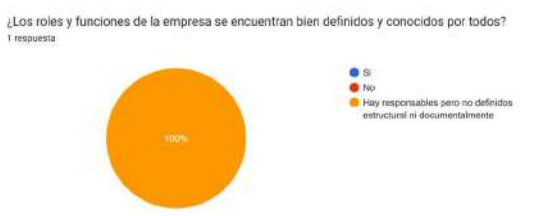
El primer tema a evaluar fue la gobernanza, gestión de riesgos y cumplimiento de la seguridad. La empresa cuenta con un solo responsable y encargado tanto de la seguridad de la información como de sistemas en general, sin existir un área o comité que evalúe en profundidad los distintos aspectos de seguridad, considerando la dimensión del grupo económico creemos que no es necesario un comité de seguridad pero recomendamos un superior que puede ser dentro de la alta gerencia para su correspondiente autorización.

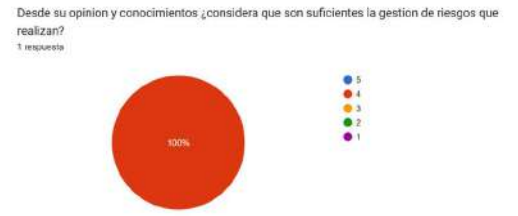


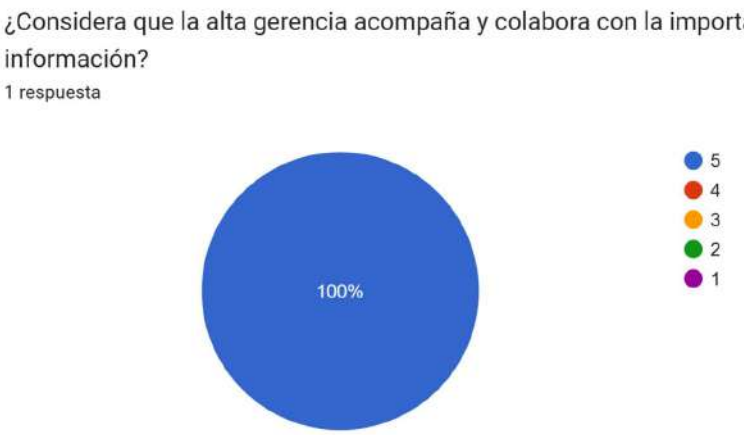


El entrevistado manifiesta que los roles y funciones relativos al tema están definidos y son conocidos por los miembros de la organización, pero estos no se encuentran documentados. Un punto a considerar como positivo es que la alta gerencia es consciente del valor de la seguridad de la información por lo que acompaña y colabora con las medidas y sugerencias que propone el encargado de seguridad. Referido a la gestión de riesgos, nos da a entender que existen procesos ante riesgos inherentes y que los mismos son considerados que son suficientes pero estos no están documentados, solo son conocidos por el responsable del área y gerencia.

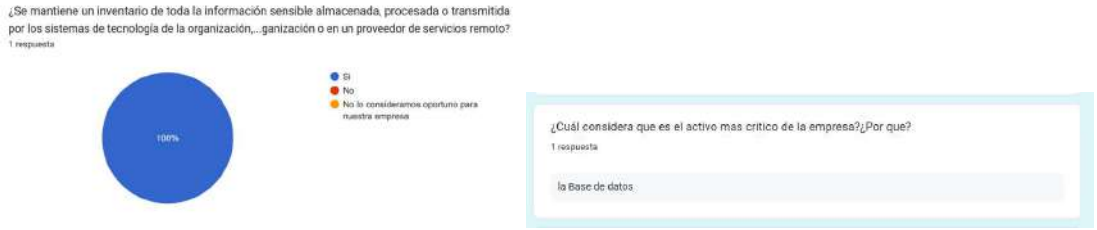
Consideramos que respecto a lo mencionado anteriormente, en el área de gobernanza y gestión, la empresa tiene un óptimo nivel de seguridad y gestión, aunque lo importante a recalcar es la ausencia de documentación de procesos. Observamos que esta documentación es vital para planes de contingencia y para que la empresa siga su rumbo sin dependencia de la persona. Otra gran ventaja de la documentación además de ser un buen punto de gestión, es que resulta práctico para la inserción de nuevos empleados, para el conocimiento de los procesos y gestiones dentro de la sociedad, sin la necesidad de estar explicando de manera verbal estos. Esto no solo aplica a documentación de los procesos sino que además de realizar organigrama dejando bien definida la estructura y limitada las funciones. CABE RECALCAR QUE ESTO ES NECESARIO PARA UN BUEN CONTROL DE GESTIÓN



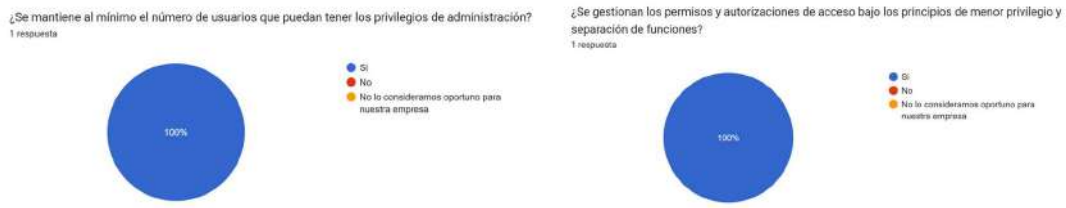




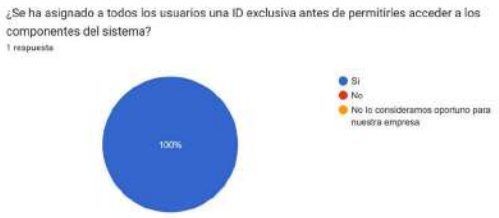
En cuanto a inventarios de la seguridad de la información se mantiene un registro de los activos de información que se posee y la información que es confidencial. Utilizan la plataforma Google Drive para mantener restringida la información de terceros. Consideramos que por el nivel de facturación y los activos de información con los que cuentan diariamente la selección es correcta siempre y cuando se le otorguen acceso a los empleados según las funciones que cumplen.

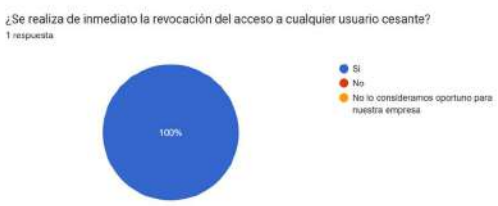


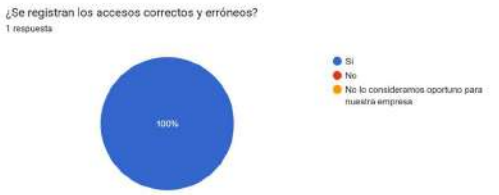
Respecto a controles de acceso al sistema, solo 3 usuarios tienen privilegios de administración, y al resto de los usuarios se les asigna un perfil y se les da accesos de acuerdo a sus funciones y cumpliendo con el concepto de mínimo privilegio, los cuales son removidos una vez que el área de recursos humanos informa la baja del empleado. La asignación de funciones no está documentada sino que es determinada por las gerencias de área al momento de incorporarse un empleado. PUNTO FUERTE y buen manejo por parte del encargado

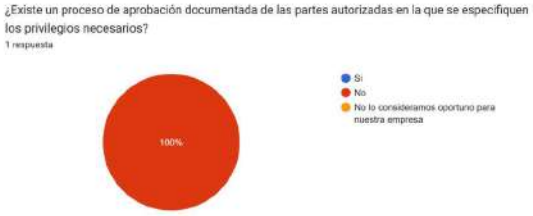


Como venimos notando desde el comienzo de nuestro análisis, la empresa se encuentra en un óptimo nivel de madurez pero no debe dejar de lado la parte documental y burocrática de la empresa, puede parecer algo menor pero deja grandes cimientos en la empresa para no depender de una sola persona y plantar las bases estructurales de su seguridad.

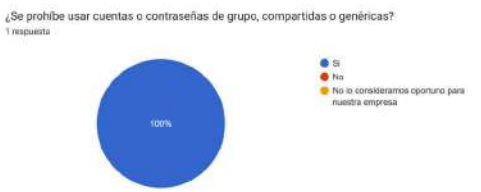


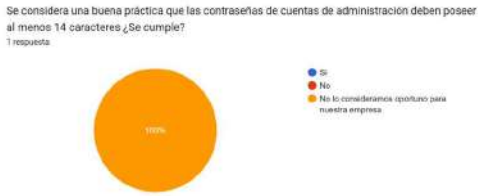




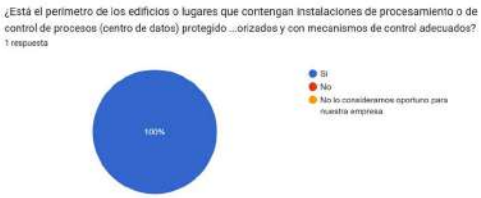


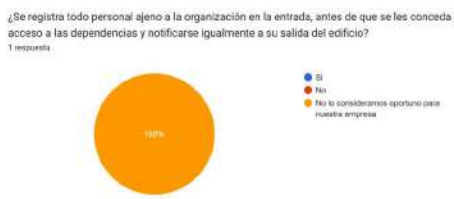
En relación a la gestión de contraseñas, la organización posee un eficiente proceso de gestión de las mismas, obligando a modificarlas cada 30 días y sin permitir poner contraseñas similares a las registradas en el historial. Como observación se destaca que no es requisito que las contraseñas tengan como mínimo 14 caracteres ni que tengan distintos tipos de caracteres (mayúsculas, números, símbolos, etc).

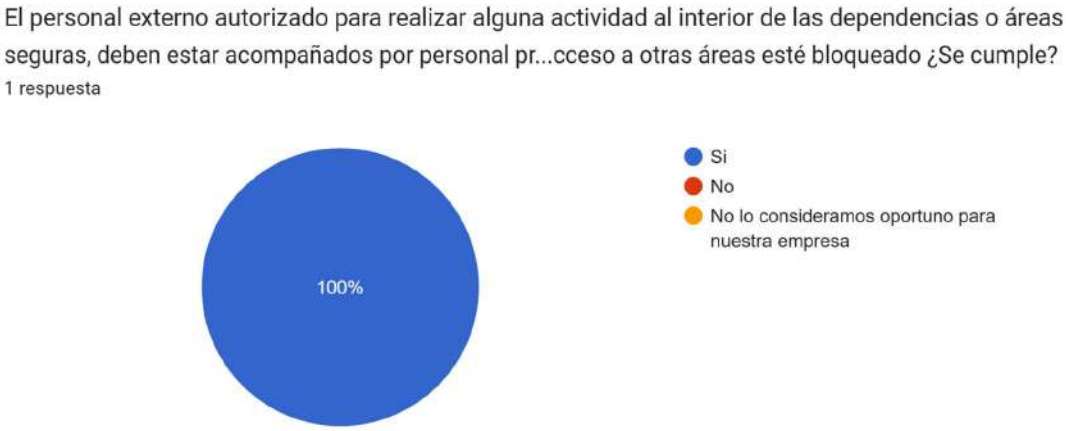




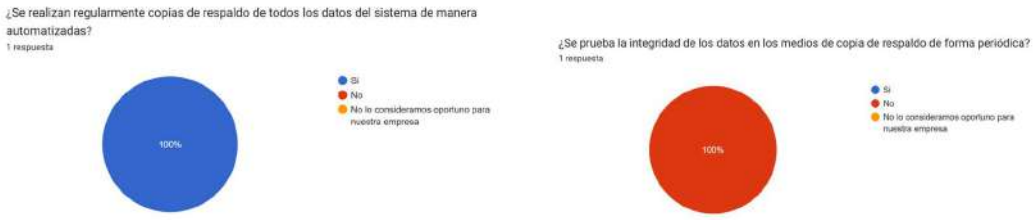
Con respecto a accesos físicos al sector donde se encuentran los activos de información, la empresa tiene protegidos sus activos, sobre todo sus servidores principales, el acceso es mediante biometría. En el caso de externos quienes tengan que realizar alguna actividad en dicho sector, los mismos no son registrados pero en todo momento son acompañados por personal propio de la organización. Consideramos oportuno el manejo en la sección de controles físicos pero también sería conveniente registrar los ingresos de personas externas a la empresa; por lo menos con un mensaje por WhatsApp, ya que podrían suceder casos de hurto en algunos casos, como ser por ejemplo que el empleado que acompañe se encuentra aliado con el tercero ingresado a la oficina.

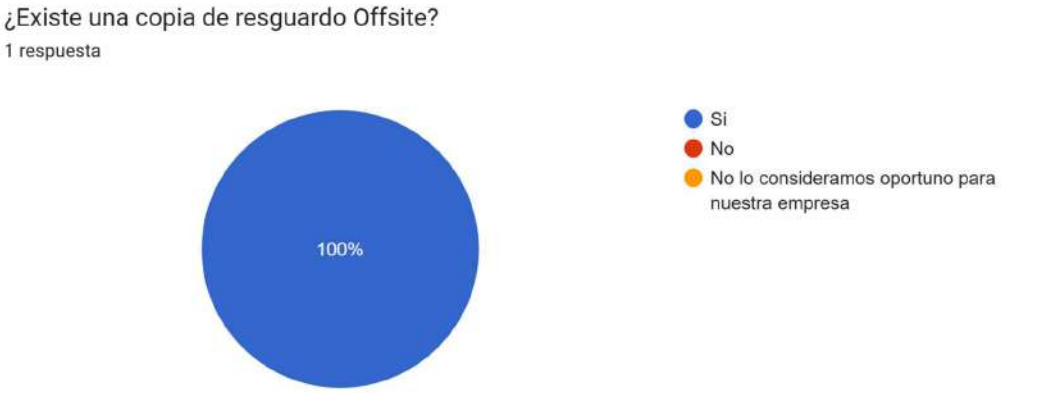






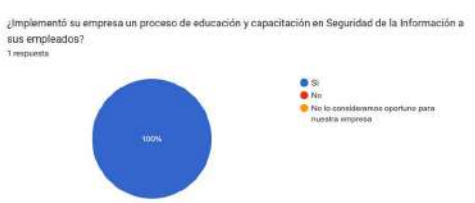
Con relación a copias de respaldo, la empresa realiza constantemente copias de seguridad de su información en un servidor paralelo para en el caso de ser infectado por malware poder recuperar su información más crítica, lo que se observa es que no se realizan pruebas de integridad de información de forma periódica. También se destaca que tienen una copia de seguridad en nube. Consideramos que no está mal la postura tomada por la empresa pero nos gustaría por lo menos revisar la integridad aunque sea mensualmente de la base de principales clientes y/o proveedores, para disminuir gastos y minimizar los daños podría realizarla a los proveedores y clientes que superen $450.000 facturación mensual

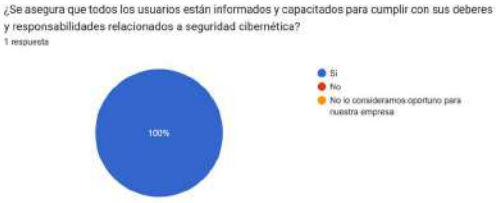


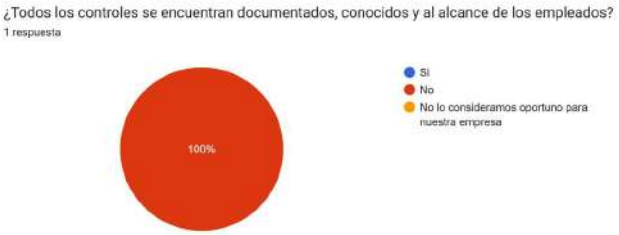


Ante la consulta de si implementan un proceso de educacion y capacitacion en seguridad de la información a sus empleados, nos contestan de que no se implementó pero si está dentro de los planes realizarlo en el corto plazo, de todos modos sus empleados están informados para evitar caer en un ciberataque, siendo el más frecuente ataques de phishing, ante los cuales los empleados

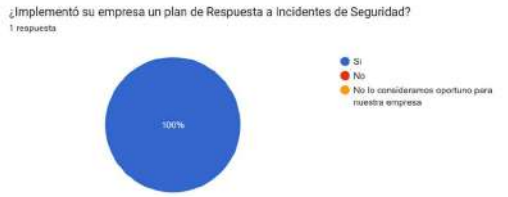
saben cómo responder, pero dicha normativa no está documentalmente informada ni al alcance para su consulta.

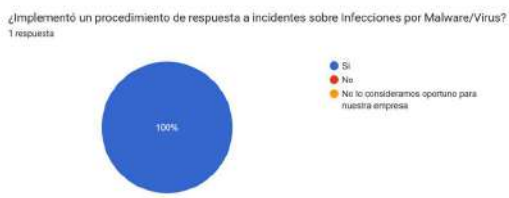


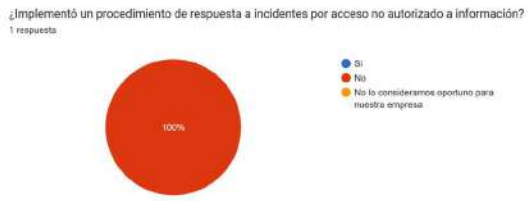


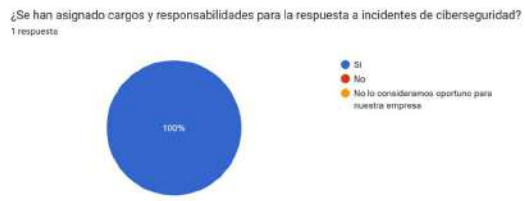


El último tema a abordar es respecto al plan de respuestas a incidentes de seguridad, el entrevistado nos respondió que sí tienen uno implementado y que fue probado ante infecciones por malware sin producir pérdidas económicas para recuperar la información robada. Las estaciones de trabajo cuentan con un sistema antimalware y los cargos y responsabilidades para respuestas a incidentes de ciberseguridad fueron asignados aunque no están documentados.









4. CONCLUSIONES

Cómo conclusión al trabajo de investigación realizado, podemos decir que nos encontramos frente a una empresa que tiene un nivel de consciencia aceptable respecto a la importancia de la seguridad de la información para el ámbito empresarial, pero notamos distintas cuestiones que deberían mejorarse para poder hablar de una empresa con un nivel de madurez de seguridad optimizado.
El punto negativo más relevante que detectamos fue la falta de documentación respaldatoria respecto a los roles y funciones del encargado de seguridad y sistemas, como así también la falta de documentación de los procesos de la empresa: como ser falta de planes de continuidad de negocio, planificación del sistema de gestión de seguridad de la información, ausencia documental del tratamiento de riesgos.
Estas debilidades pueden encontrar sus causas en tener las tareas de seguridad muy centralizadas en personas específicas de la gerencia, que conocen sus funciones y saben ejecutarlas correctamente, pero evidencian no tener dichos procesos correctamente detallados y documentados. También se puede deber a una falta de consciencia respecto a la importancia de documentar los procesos que se realizan día a día en la empresa. Esto nos parece algo que se debería corregir lo antes posible para poder hablar de una correcta cultura de seguridad de la información a nivel organizacional.
Dentro de los puntos más fuertes de la gestión de seguridad que encontramos, destacamos:

-Registro y clasificación de los activos de información.
-Accesos a información sensible sólo para personal autorizado.
-Correcto manejo de contraseñas.
-Controles físicos de seguridad.
-Copias de seguridad de la base de datos.
-Empleados informados sobre ataques de ciberseguridad.
-Procesos de respuesta a incidentes de seguridad implementados.

En síntesis, respecto a lo que pudimos evaluar a partir de nuestro conocimiento de la empresa en base a la entrevista y a la información que nos brindaron sus empleados, podemos concluir que nos encontramos ante una empresa con un nivel de madurez L3: proceso definido.
Esto basándonos en la escala de madurez para medir los aspecto organizativos, que “recoja en forma de factor corrector la confianza que merece el proceso de gestión” en Magerit v 3.0. La escala empleada sería la siguiente:

factor	nivel	significado
0%	**L0**	inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	**L5**	optimizado

Consideramos que si la organización realiza las correcciones recomendadas en el análisis de los resultados de la entrevista, la empresa podría ubicarse en un nivel L4 gestionado y medible.

5. REFERENCIAS BIBLIOGRÁFICAS

- Controles CyS- Campus
- Entrevista documentada por GOOGLE FORM con el encargados en sistemas
- Entrevistas a empleados
- Contenidos aprendidos a lo largo del cursado
- Gestión de riesgos- INCIBE
- Protección de la información - INCIBE
- Magerit - Versión 3.0 Metodología de análisis y gestión de riesgos de los Sistemas de Información

6. ANEXOS

Tablas y gráficos realizados en base a los resultados de la entrevista.

Cuestionario: https://forms.gle/Rp6Q9bBMySEhVaK19
Respuestas: Respuestas a cuestionario SyC