**Autoevaluación en Ciberseguridad**

**Considerando que la ciberseguridad se ha tomado la agenda y pasado a ser un tema candente y prioritario, la Cámara de Comercio de Santiago (CCS) presenta esta autoevaluación elaborada por la Cámara de Comercio Internacional (ICC), a la cual representa en Chile, que permite a las empresas realizar un autoanálisis de los ciberiesgos que enfrentan.**

**Autoevaluación**

El cuestionario de autoevaluación se puede utilizar como una lista de tareas de las empresas que están empezando sus iniciativas de seguridad de la información y quieren usar la información como base para la planiﬁcación de sus capacidades de resiliencia cibernética.

Para cada una de las siguientes preguntas, las empresas deben identiﬁcar, entre las opciones propuestas, la que le parezca el reﬂejo más exacto de las prácticas actuales. A cada una de las opciones le ha sido dado un color, donde:

**X** Esta es la respuesta menos deseable; claramente debe considerarse una mejora.

! Es posible una mejora adicional para proteger mejor la empresa.

**✓**  Es el mejor reﬂejo de capacidad de recuperación frente a las ciberamenazas

**Cuestionario**

**1- ¿Evalúan el manejo de la información sensible en su empresa?**

**X** No, pero tenemos un firewall que nos protege del robo de información.

! Sí, entendemos la importancia de nuestra información e implementamos medidas generales de seguridad

**✓**Sí y tenemos un modelo de clasificación de información y sabemos dónde está almacenada y procesada nuestra información sensible. Implementamos medidas de seguridad basadas en el nivel de importancia de la información.

|  |  |  |
| --- | --- | --- |
| Las siguientes preguntas se ofrecen como una lista de veriﬁcación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso. | **SÍ** | **NO** |
| ¿Están sus datos sensibles identiﬁcados y clasiﬁcados? |  |  |
| ¿Está consciente de su responsabilidad con respecto a los datos identiﬁcados como sensibles? |  |  |
| ¿Los datos más sensibles están altamente protegidos o cifrados? |  |  |
| ¿La gestión de la información privada del personal queda cubierta por los procedimientos? |  |  |
| ¿Son todos los empleados capaces de identiﬁcar y proteger correctamente los datos sensibles y no sensibles? |  |  |

**2- ¿Realiza evaluaciones de riesgos relacionados con la seguridad de la información?**

X Nosotros no realizamos evaluaciones de riesgo.

! Evaluamos riesgos, pero no sobre ningún tema relacionado especíﬁcamente con la seguridad de la información.

**✓**Llevamos a cabo evaluaciones de riesgos sobre asuntos especíﬁcos de seguridad de la información.

|  |  |  |
| --- | --- | --- |
|  | **SÍ** | **NO** |
| ¿Ordena los resultados del análisis de vulnerabilidades desde alto riesgo a bajo riesgo? |  |  |
| ¿Son identiﬁcados los eventos que podrían causar interrupciones en los procesos de negocio y está evaluado el impacto que potencialmente producirían dichas interrupciones? |  |  |
| ¿Tiene un plan de continuidad de negocio que se prueba y se actualiza de forma regular? |  |  |
| ¿Realiza una evaluación periódica de riesgos  para actualizar el nivel de protección de los datos y la información? |  |  |
| ¿Están las áreas de riesgo identiﬁcadas a lo largo de sus procesos de negocio para evitar la corrupción en el tratamiento de la información o su mal uso deliberado? |  |  |

**3-¿A qué nivel está implementado el gobierno de seguridad de la información?**

X No se ha implantado un gobierno de seguridad de la información.

! La gobernanza de la seguridad de información se hace en el departamento de TI ya que es donde hace falta que la información esté protegida.

**✓**La gobernanza de la seguridad de información se instala a nivel corporativo para asegurar su impacto en toda la empresa.

|  |  |  |
| --- | --- | --- |
|  | **SÍ** | **NO** |
| ¿Los miembros del comité de dirección y el CEO destinan un presupuesto a seguridad de la información? |  |  |
| ¿La seguridad de la información forma parte de la gestión de riesgos que hacen los directores? |  |  |
| ¿La dirección aprueba la política de seguridad de la información de la empresa y la comunica a los empleados por un medio adecuado? |  |  |
| ¿Están regularmente informados los miembros del comité de dirección y del equipo gestor de la empresa acerca de los últimos avances en políticas, normas, procedimientos y directrices seguridad de la información? |  |  |
| ¿Hay por lo menos un oﬁcial perteneciente al equipo gestor que esté a cargo de la protección de los datos de carácter personal y la privacidad? |  |  |

**4-¿Dispone de un equipo de seguridad de la información o una función dedicada dentro de su empresa?**

**X** No tenemos un equipo de seguridad de la información, ni funciones o responsabilidades especíﬁcas sobre seguridad de la información.

! No tenemos un equipo de seguridad de la información, pero hemos deﬁnido las funciones y responsabilidades especíﬁcas de seguridad de información dentro de la empresa.

**✓**Tenemos un equipo de seguridad de la información o una función dedicada a la seguridad de la información.

|  |  |  |
| --- | --- | --- |
|  | **SI** | **NO** |
| ¿Tiene identiﬁcado un especialista en seguridad de la información o un equipo que coordine internamente el conocimiento y proporcione ayuda al equipo gestor en la toma de decisiones? |  |  |
| ¿El especialista identiﬁcado o equipo de seguridad de la información es responsable de revisar y actualizar sistemáticamente la política de seguridad de la información basada en cambios signiﬁcativos o incidentes? |  |  |
| ¿Tiene el especialista identiﬁcado, o el equipo de seguridad, la suﬁciente visibilidad y apoyo para intervenir en cualquier iniciativa relacionada con la información en la empresa? |  |  |
| ¿Existen diferentes gestores responsables para distintos tipos de datos? |  |  |
| ¿Se revisan regularmente, por parte de un organismo independiente o de un auditor, la viabilidad y la eﬁcacia de la política de seguridad de la información, así como la eﬁcacia del equipo de seguridad de la información? |  |  |

**5-¿De qué manera trata su empresa los riesgos de seguridad de información relacionados con proveedores que pueden acceder a su información conﬁdencial?**

**X** Tenemos una relación basada en la conﬁanza mutua con nuestros proveedores.

! Para algunos contratos se incluyen cláusulas relacionadas con la seguridad de la información.

**✓**Tenemos procesos que validan el acceso de los proveedores y pautas especíﬁcas de seguridad que se comunican y son ﬁrmados por nuestros proveedores.

|  |  |  |
| --- | --- | --- |
|  | **SI** | **NO** |
| ¿Están los contratistas y proveedores identiﬁcados con una tarjeta de identiﬁcación con una foto reciente? |  |  |
| ¿Tiene usted políticas que abordan la veriﬁcación de antecedentes para contratistas y proveedores? |  |  |
| ¿El acceso a las instalaciones y los sistemas de información se terminan automáticamente cuando un contratista o proveedor termina su misión? |  |  |
| ¿Saben los proveedores cómo y a quién informar de inmediato en su empresa sobre la pérdida o robo de información? |  |  |
| ¿Se asegura su empresa de que los proveedores tienen su software y aplicaciones actualizadas con los parches de seguridad? |  |  |
| ¿Los requerimientos de seguridad están claramente deﬁnidos en los acuerdos contractuales con contratistas/proveedores? |  |  |

**6-¿Evalúa su compañía de forma regular la seguridad de los equipos informáticos y de la red?**

**X** No realizamos auditorías o pruebas o de intrusión para evaluar nuestra seguridad en ordenadores y redes.

! No tenemos un enfoque sistemático para la realización de auditorías de seguridad y / o pruebas de intrusión, pero ejecutamos alguna *ad-hoc* cuando resulta necesario.

**✓**Las auditorías regulares de seguridad y/o pruebas de intrusión son parte sistemática de nuestro enfoque para evaluar la seguridad de ordenadores y de la red.

|  |  |  |
| --- | --- | --- |
|  | **SI** | **NO** |
| ¿Realiza pruebas de forma regular y mantiene un registro de las amenazas identiﬁcadas? |  |  |
| ¿Tiene procedimientos para evaluar las amenazas humanas a sus sistemas de información, incluyendo la falta de honradez, la ingeniería social y el abuso de conﬁanza? |  |  |
| ¿Solicita su empresa los informes de auditoría de seguridad de la información a sus proveedores de servicios? |  |  |
| ¿Se evalúa también durante las auditorías de seguridad la utilidad de cada tipo de dato almacenado? |  |  |
| ¿Audita usted sus procesos y procedimientos de cumplimiento de las políticas y normas establecidas en la empresa? |  |  |

**7-Cuando se introducen nuevas tecnologías, ¿evalúa su empresa los riesgos potenciales para la seguridad de la información?**

**X** La seguridad de la información no se tiene en cuenta en el proceso de implantación de nuevas tecnologías.

! La seguridad de la información se implementa *ad-hoc* en el proceso de adopción de nuevas tecnologías, sólo cuando resulta necesario.

**✓** La seguridad de la información está incluida en el proceso de implementación de las nuevas tecnologías.

|  |  |  |
| --- | --- | --- |
|  | **SI** | **NO** |
| Al considerar la aplicación de nuevas tecnologías, ¿evalúa su impacto potencial en la política de seguridad de la información que tiene establecida su empresa? |  |  |
| ¿Existen medidas de protección para reducir el riesgo en la aplicación de nuevas tecnologías? |  |  |
| ¿Están documentados los procesos para aplicar nuevas tecnologías? |  |  |
| En la aplicación de nuevas tecnologías ¿puede su empresa conﬁar en suministradores que garanticen la colaboración y el intercambio de información crítica de seguridad? |  |  |
| ¿Se considera a menudo la política de seguridad de la información de su empresa como una barrera a las oportunidades tecnológicas? |  |  |
| ¿Gestiona la empresa las nuevas tecnologías utilizando metodología de seguridad en el desarrollo de sistemas dentro del ciclo de vida de los sistemas? |  |  |

**8-¿Proporciona su empresa entrenamiento en seguridad de información?**

**X** Conﬁamos en nuestros empleados y no consideramos que las orientaciones sobre seguridad de la información sean un valor añadido.

! Sólo nuestro personal de TI recibe capacitación especíﬁca para proteger nuestra TI.

**✓**Regularmente se organizan sesiones de sensibilización de seguridad de información para todos los empleados.

|  |  |  |
| --- | --- | --- |
|  | **SI** | **NO** |
| ¿Se adaptan algunas de las sesiones de concienciación sobre seguridad de información al ámbito de actividad de los empleados? |  |  |
| ¿Se enseña a los empleados a estar atentos ante posibles brechas de seguridad de información? |  |  |
| ¿Dispone su empresa de una guía para que los usuarios reporten debilidades de seguridad en, o amenazas hacia sistemas o servicios? |  |  |
| ¿Saben los empleados manejar correctamente los datos de tarjetas de crédito y datos de carácter personal privados? |  |  |
| ¿El personal ajeno y otros usuarios (en su caso) reciben también apropiada capacitación en seguridad de información y actualizaciones periódicas en las políticas y procedimientos de la organización? |  |  |

**9-¿Cómo se usan las contraseñas en su empresa?**

**X** Compartimos las contraseñas con otros colegas y/o no existe una política para el uso seguro de las contraseñas o para el cambio periódico de éstas

! Todos los empleados, incluyendo al equipo gestor, tienen contraseñas únicas, pero no se obliga a elegirlas según reglas de mínima complejidad. El cambio de contraseñas es opcional, no es obligatorio.

**✓**Todos los empleados, incluyendo al equipo gestor, tienen una clave personal que debe cumplir con unos requisitos especíﬁcos y debe ser cambiada regularmente.

|  |  |  |
| --- | --- | --- |
|  | **SI** | **NO** |
| ¿Su empresa ha establecido el cumplimiento obligado de una política de contraseñas aceptada globalmente para todos los activos de la empresa? |  |  |
| ¿Puede usted asegurar lo siguiente acerca de todas las contraseñas en su empresa?  • No se almacenan en archivos de fácil acceso;  • No son débiles o en blanco o se dejan con la conﬁguración por defecto;  • Se cambian, especialmente en los dispositivos móviles. |  |  |
| ¿Se siente bien protegido contra el acceso físico no autorizado a los sistemas? |  |  |
| ¿Son los usuarios y los suministradores conscientes de su responsabilidad para proteger equipos desatendidos (por ejemplo, cerrando las sesiones cuando se marchan al ﬁnalizar su trabajo)? |  |  |
| ¿Se ha enseñado a los empleados cómo reconocer los trucos de ingeniería social que se utilizan para engañar a la gente para que divulguen detalles de seguridad y cómo deben reaccionar ante esta amenaza? |  |  |

**10-¿Existe una política de empresa para un uso aceptable de Internet y de las redes sociales?**

**X** No, no existe una política para el uso aceptable de Internet.

! Sí, existe y está disponible en una ubicación centralizada accesible a todos los empleados, pero no ha sido ﬁrmado por los empleados.

**✓**Sí, una política para el uso apropiado Internet es parte del contrato laboral / todos los empleados han ﬁrmado la política de uso aceptable.

|  |  |  |
| --- | --- | --- |
|  | **SI** | **NO** |
| ¿Existen directrices y procesos generales de comunicación para los empleados en la empresa, que incluyen la relación con la prensa y los medios de comunicación? |  |  |
| ¿Hay un proceso disciplinario para los empleados que violen las pautas de comunicación de la empresa? |  |  |
| ¿Monitoriza Internet un determinado gerente de comunicación o su equipo, con el ﬁn de evaluar los riesgos a la reputación y la posición de su empresa? |  |  |
| ¿Ha evaluado su empresa la responsabilidad por los actos de los empleados u otros usuarios internos o atacantes de los sistemas que puedan utilizarlos para perpetrar actos ilícitos? |  |  |
| ¿Ha tomado medidas su empresa para evitar que un empleado u otro usuario interno ataque a otros sitios? |  |  |

**11-¿Su empresa mide, reporta y hace seguimiento de asuntos relacionados con Seguridad de la Información?**

**X** Nosotros no controlamos, ni informamos o hacemos seguimiento sobre la eﬁcacia y la adecuación de las medidas de seguridad implementadas.

! Nuestra empresa ha implementado herramientas y métodos para monitorizar, reportar y hacer seguimiento de la eﬁcacia y la adecuación de una selección de medidas de seguridad implementadas.

**✓**Nuestra empresa ha puesto en marcha las herramientas y los métodos necesarios para monitorizar, reportar y hacer seguimiento de la eﬁcacia y la adecuación de todas nuestras medidas de seguridad implementadas.

|  |  |  |
| --- | --- | --- |
|  | **SI** | **NO** |
| ¿Se conservan las trazas de auditoría y registros relativos a los incidentes y se desarrollan acciones proactivas para que el incidente no vuelva a ocurrir? |  |  |
| ¿Veriﬁca su empresa el cumplimiento de los requisitos legales y regulatorios  (por ejemplo los de privacidad de datos)? |  |  |
| ¿Ha desarrollado su empresa alguna herramienta propia para ayudar al equipo gestor en la evaluación de la postura de seguridad y que permita a la compañía acelerar su capacidad para mitigar riesgos potenciales? |  |  |
| ¿Existe en su empresa una hoja de ruta o plan de seguridad de información que incluya objetivos, evaluación de los avances y posibles oportunidades de colaboración? |  |  |
| ¿Se reportan los informes sobre incidentes a las autoridades y otros grupos de interés como asociaciones de empresas del sector? |  |  |

**12-¿Cómo se mantienen actualizados los sistemas de su empresa?**

**X** Contamos con gestión automática de parches, proporcionada por el vendedor, para la mayoría de nuestras soluciones.

! Las actualizaciones de seguridad se aplican cada mes de forma sistemática.

**✓**Tenemos un proceso de gestión de vulnerabilidades continuamente busca información sobre las posibles vulnerabilidades (por ejemplo a través de una suscripción a un servicio que envía automáticamente avisos de nuevas vulnerabilidades) y aplicamos parches basados en los riesgos que mitigan.

|  |  |  |
| --- | --- | --- |
|  | **SI** | **NO** |
| ¿Es el análisis de vulnerabilidades una tarea de mantenimiento programada regularmente en la empresa? |  |  |
| ¿Se revisan y prueban las aplicaciones después de cualquier cambio en el sistema operativo? |  |  |
| ¿Pueden los usuarios comprobar por sí mismos si existen aplicaciones sin parches? |  |  |
| ¿Están los usuarios conscientes de que también tienen que mantener el sistema operativo y las aplicaciones actualizadas incluyendo el software de seguridad de sus dispositivos móviles? |  |  |
| Están los usuarios entrenados para reconocer un mensaje auténtico de advertencia, como la solicitud de permiso para actualizar (por ejemplo distinguiéndolo de solicitudes de falsos antivirus), y a notiﬁcarlo adecuadamente al equipo de seguridad si sucede algo malo o cuestionable? |  |  |

**13-¿Se revisan y gestionan de forma regular los derechos de acceso de los usuarios a las aplicaciones y los sistemas?**

**X** Los derechos de acceso a las aplicaciones y los sistemas no revisan ni se retiran consecuentemente.

! Los derechos de acceso a las aplicaciones y los sistemas sólo se eliminan cuando un empleado deja la compañía.

**✓**Se ha establecido una política de control de acceso con revisiones periódicas de los derechos de acceso asignados a los usuarios para todas las aplicaciones relevantes del negocio y los sistemas de que las soportan.

|  |  |  |
| --- | --- | --- |
|  | **SI** | **NO** |
| ¿Están los accesos a sistemas de información y recursos limitados por política y procedimientos? |  |  |
| ¿Su empresa dispone de una política de privacidad donde se declara el tipo de datos personales que se recogen (por ejemplo, en el caso de sus clientes: direcciones postales, direcciones de correo electrónico, historial de navegación, etc.), y las ﬁnalidades para la que se aplican los tratamientos de dichos datos? |  |  |
| ¿Las políticas y procedimientos especiﬁcan los métodos utilizados para controlar el acceso físico a zonas seguras tales como cerraduras de puertas, sistemas de control de acceso físico o videovigilancia? |  |  |
| ¿Se le retira automáticamente la autorización de acceso a las instalaciones y los sistemas de información cuando se desvincula a un empleado? |  |  |
| ¿Están clasiﬁcados los datos por razón de su sensibilidad (por ejemplo, altamente conﬁdencial, sensible uso interno) y sus usuarios ﬁguran en una lista de control de acceso? |  |  |
| ¿Está regulado el acceso remoto a los sistemas de información de la empresa? |  |  |

**14-En su empresa, ¿pueden los empleados usar sus propios dispositivos personales, como teléfonos móviles y tabletas, para almacenar o transferir información de la empresa?**

**X** Sí, podemos almacenar o transferir información de la empresa en los dispositivos personales sin aplicar medidas de seguridad adicionales.

! Existe una política que prohíbe el uso de dispositivos personales para almacenar o transferir información de la compañía, pero técnicamente es posible hacerlo sin que tengamos que aplicar medidas de seguridad adicionales.

**✓**Los dispositivos personales sólo pueden almacenar o transferir información de la empresa después de aplicar medidas de seguridad en el dispositivo personal y/o cuando se nos ha proporcionado una solución profesional.

|  |  |  |
| --- | --- | --- |
|  | **SI** | **NO** |
| ¿Su empresa confía en la política ampliamente aceptada de “traiga usted su propio dispositivo (Bring Your Own Device)”? |  |  |
| ¿Están los dispositivos móviles protegidos contra usuarios no autorizados? |  |  |
| ¿Están todos los dispositivos y conexiones permanentemente identiﬁcados en la red? |  |  |
| ¿Se han instalado el cifrado en cada dispositivo móvil para proteger la conﬁdencialidad e integridad de los datos? |  |  |
| ¿Es consciente el nivel corporativo de que mientras el empleado puede ser responsable de un dispositivo, la compañía sigue siendo responsable de los datos? |  |  |

**15-¿Su empresa ha tomado medidas para prevenir la pérdida de información almacenada?**

**X** No tenemos ningún proceso de copia/restauración de seguridad.

! Tenemos un proceso de copia/restauración de seguridad, pero no se realizan pruebas de restauración.

**✓**Tenemos un proceso de copia/restauración de seguridad, que incluye pruebas de restauración/ resiliencia. Tenemos copias de respaldo almacenadas en otro lugar seguro o utilizamos otras soluciones de alta disponibilidad.

|  |  |  |
| --- | --- | --- |
|  | **SI** | **NO** |
| ¿Entre sus empleados existe personal suﬁciente capaz de crear copias de seguridad y archivar ﬁcheros? |  |  |
| ¿Están protegidos los equipos contra fallos de energía mediante el uso de fuentes de alimentación permanente como alimentación múltiple, fuentes de alimentación ininterrumpida (UPS), generadores de emergencia, etc.? |  |  |
| ¿Se prueban con regularidad los medios de copia de seguridad para asegurarse de que podrán ser restaurados dentro del plazo de tiempo ﬁjado en el procedimiento de recuperación? |  |  |
| ¿Se aplican en su empresa procedimientos de reporte de equipos móviles perdidos o robados? |  |  |
| ¿Están los empleados capacitados sobre qué hacer si se borra accidentalmente la información y cómo recuperar la información en caso de desastre? |  |  |
| ¿Se han implementado medidas para proteger tanto la conﬁdencialidad como la integridad de las copias de seguridad en su lugar de almacenamiento? |  |  |

**16-¿Está su empresa preparada para manejar un incidente de seguridad de información?**

**X** No tendremos ningún incidente. En caso de que lo tengamos, nuestros empleados son lo suﬁcientemente competentes para hacerles frente.

! Tenemos procedimientos de gestión de incidentes, sin embargo, no están adaptados para manejar incidentes de seguridad de la información.

**✓**Tenemos un proceso dedicado para manejar incidentes de seguridad de la información, con los mecanismos necesarios de comunicación y escalado. Nos esforzamos para manejar incidentes tan eﬁcientemente como nos es posible, de modo que aprendemos cómo protegernos mejor a nosotros mismos en el futuro.

|  |  |  |
| --- | --- | --- |
|  | **SI** | **NO** |
| ¿Tienen en cuenta sus procesos diferentes tipos de incidentes, que van desde una denegación de servicio a la violación de la conﬁdencialidad, etc., y las forma de manejarlos? |  |  |
| ¿Su empresa tiene un plan de comunicación en la gestión de incidentes? |  |  |
| ¿Sabe usted a qué autoridades tiene que notiﬁcar y cómo hacerlo en el caso de un incidente? |  |  |
| ¿Su empresa dispone de información de contactos identiﬁcados y ordenados según cada tipo de incidente? |  |  |
| ¿Usted confía en un gestor de comunicación interna para contactar con los empleados y sus familias durante la gestión de incidentes? |  |  |
| ¿Existe un proceso de lecciones aprendidas con el ﬁn de hacer mejoras en la gestión de incidentes después de que haya ocurrido un incidente de seguridad de información? |  |  |