Seguridad de la información

1. Objetivo

Asegurar que la información (obtenida, gestionada y/o generada) esté protegida contra modificaciones no planeadas, realizadas con o sin intención, que sea accedida solo por aquellos que tengan una necesidad legitima para realizar las funciones de la organización; que esté disponible cuando sea requerida y para que sea utilizada con los propósitos con que fue adquirida.

2. Alcance.

La política de seguridad de la información da las directrices requeridas para la implementación de un modelo de seguridad confiable y flexible. Aplica para todos los niveles de la organización (usuarios: incluye empleados y partners), entes de control, entidades relacionadas que accedan a la información de forma interna o externa a cualquier activo independiente de su ubicación.

Aplica para toda la información obtenida, gestionada y/o generada en soporte de la organización, cualquiera que sea el medio, formato, presentación o lugar (física o virtual) en el cual se encuentre.

3. Definiciones

Información: La información es algo dicho o escrito como informes, conocimiento y datos; que a su vez se difunde de varias maneras, tales como comunicación oral, documentos escritos o por medios electrónicos. (Adaptado del Min Tic)

Información crítica: es el activo más importante de la organización ya que esta garantiza la continuidad del negocio, por lo tanto, la empresa debe garantizar su Integridad, Confidencialidad, Disponibilidad y Privacidad, ya que si se pone en riesgo de pérdida puede llegar a afectar su imagen financiera y legal (www.estrategiaynegocios.net).

Confidencialidad: Se refiere al impacto en la institución en caso de que información crítica llegue a manos equivocadas. Se trata de un aspecto que tiene que ver con la protección de datos contra accesos no autorizados y para protegerlos de una posible corrupción durante todo su ciclo de vida.

Seguridad de datos incluye conceptos como encriptación de datos, tokenización y prácticas de gestión de claves que ayudan a proteger los datos en todas las aplicaciones y plataformas de una organización. (www.powerdata.es/)

Controles de seguridad: para definir los objetivos principales en la implementación de una seguridad apropiada, se debe considerar las siguientes categorías (web.mit.edu):

a. Controles físicos: es la implementación de medidas de seguridad en una estructura definida para prevenir o detectar acceso no autorizado a material confidencial.
b. Controles técnicos: uso de la tecnología para controlar el acceso y uso de datos confidenciales a través de una estructura física y sobre la red.
c. Controles administrativos: son aquellos que defines los factores humanos de la seguridad, incluye todos los niveles del personal dentro de la organización y define los usuarios y sus accesos a los recursos, dependiendo de su necesidad de uso sobre estos.

Disponibilidad: Se refiere al Impacto en la institución en caso de que la información no esté disponible para ser utilizada. El no disponer de información crítica cuando es

requerida, pudiera resultar en una perdida financiera significativa para la organización. Por ejemplo, si un servidor no se encuentra disponible por un periodo de tiempo, o se sufre la pérdida de un archivo crítico debido a errores humanos, puede ocasionar que la institución no pueda ofrecer sus servicios a sus usuarios, ocasionándole pérdida de imagen y credibilidad.

Recursos de Información: Todas las categorías de información, que incluyen: archivos, grupos de datos, equipos (incluso los sistemas de computación personal), instalaciones y el software propietario o licenciado de CertMind.

Seguridad de la información: La protección de la información contra el acceso no autorizado accidental o intencional, su modificación, destrucción o publicación.

Internet: El Internet es la conexión lógica de múltiples redes de comunicaciones, las cuales utilizan como estándar el protocolo TCP/IP para comunicarse y compartir datos entre dichas redes de acceso público. (https://definicion.de)

Integridad: Se refiere al Impacto en la institución en caso de que no se utilice la información correcta. Cuando la integridad de la información se pierde, los usuarios pueden perder su confianza, pieza clave dentro de la relación con los clientes.

Responsable de la Información: Un individuo o unidad organizacional que tiene responsabilidad por clasificar y tomar decisiones de control con respecto al uso de su información.

4. Responsabilidades y autoridades

Función	Descripción

Responsable de la información	• Debe implementar la política de seguridad en la organización, para lo cual debe conocer el valor de la información
Usuarios (estudiantes y partners)	• Son responsables y deben proteger los activos de la información de CertMind por medio del cumplimiento de la política de seguridad de la información, de igual forma estarán atentos a identificar y reportar cualquier incumplimiento a la norma o procedimiento establecido.

5. Descripción de las políticas

5.1. Protección de la información.

La información del negocio es un activo vital de CertMind, por lo tanto, debe ser protegida.

La seguridad de la información del negocio es el conjunto de medidas de protección que toma CertMind en **contra de la divulgación, modificación o uso indebido, violación o hurto, sustracción, interceptación o destrucción maliciosa o accidental** de su información. Dichas medidas serán tomadas con base en el valor relativo de la información y el riesgo en que se pueda ver comprometida.

Los responsables de la información deben asegurarse de que la información del negocio cuenta con la protección apropiada para que se conserve su integridad, confidencialidad, disponibilidad y privacidad de la información.

CertMind debe proveer los medios necesarios para asegurase de que cada usuario proteja y preserve los activos de la información de una manera consiente y confiable.

Cualquier persona que intente inhabilitar, vencer o sobrepasar cualquier control de seguridad de forma no autorizada será sujeto a una acción disciplinaria.

Recognizes

5.2. Protección de la propiedad intelectual

La propiedad intelectual e industrial sobre patentes, derechos de autor, invenciones o información, permanecerá dentro de CertMind. de igual forma, la organización respetará los derechos de autor y licencias de uso, para lo cual solamente software licenciado y probado debe ser cargado en los sistemas de CertMind.

La propiedad intelectual corresponde a los derechos legales que tiene una institución como resultado de su actividad intelectual en el campo de la industria. Esta esta relacionada con las creaciones de la mente: las invenciones, diseños, la información, los símbolos, los nombres, las imágenes, los dibujos y los modelos utilizados en el comercio (https://www.wipo.int/about-ip/es/).

Todo el material que sea desarrollado por cualquier integrante de la entidad se considera que es propiedad intelectual de CertMind y que es de uso exclusivo por la entidad, por lo tanto, debe ser protegido contra un develado, descubrimiento o uso que disminuya la competitividad de CertMind.

Cualquier software instalado en los sistemas de computo de CertMind debe tener una licencia valida. Cada licencia debe ser almacenada en un repositorio central. Esto incluye programas “freeware” y “shareware” obtenidos de Internet, software autorizado por Proveedores y/u otras fuentes. Cualquier software que no esté dentro de los estándares debe ser aprobado por la gerencia estratégica, para que pueda ser utilizado en el ambiente de la Compañía.

5.3. Cumplimiento y regulaciones.

CertMind debe cumplir con las regulaciones aplicables al país en donde se esté prestando el servicio.

La inclusión de las regulaciones de los países en los que se opere será objeto de análisis, evaluación, aprobación, desarrollo y difusión. Si llegará a existir algún conflicto entre regulaciones, se seleccionará la más restrictiva.

De igual forma, y con el fin de mantener un buen nivel de seguridad, esta política se apoyará bajo las mejores prácticas de seguridad de la información.

5.4. Administración del riesgo de seguridad de la información.

Los riesgos a los que está expuesta la información de CertMind deben ser identificados, evaluados y mitigados de acuerdo con su valor, probabilidad de ocurrencia e impacto en el negocio.

La información del negocio (exámenes, plataformas, materiales, listas de asistencia, bases de datos de clientes, información legal y financiera e informes) se debe proteger de acuerdo con esta política. Por lo tanto, ante cualquier cambio en los procesos, se debe realizar un análisis del impacto en el negocio y en la seguridad de la información.

Cada usuario de la información debe estar enterado de los riesgos que se pueden presentar en el desarrollo de sus actividades, por lo tanto, deberá reportar inmediatamente cualquier sospecha u observación de un incidente a la seguridad de la información.

5.5. Cumplimiento y responsabilidades de la seguridad de la información

Los contratos de los empleados deben incluir cláusulas que especifiquen las responsabilidades que tienen con la información de CertMind. Adicionalmente, se deben especificar claramente dentro de sus funciones las responsabilidades correspondientes a la seguridad de la Información y al cumplimiento del Código de Ética y Conducta; haciéndole conocer las consecuencias en caso de no ser seguidas y cumplidas.

5.6. Terceros que acceden a la información de forma local o remota.

El uso de los recursos de información de CertMind por personal de Terceros, Entidades Relacionadas y Partners de CertMind, ya sea local o remotamente, debe ser formalizado por medio de acuerdos que hagan obligatorio el cumplimiento de la presente Política.

En el contrato de servicios se deben hacer referencia a la confidencialidad y buen uso de la información. En aquellos en los que se le delegue a terceros, servicios del negocio o tecnológicos, se debe incluir información adicional que detalle su compromiso en el cuidado de los recursos de información de CertMind y las penas a que estarían sujetos en caso de incumplirlos.

Para el desarrollo de los procesos, el Tercero o Entidad Relacionada cuenta con un representante dentro de CertMind (Profesional en ventas), que vela por el correcto uso y la protección de los recursos de información del negocio. Éste será responsable por la actividad de dichos funcionarios durante la vigencia del contrato.

5.7. Identificación y Autenticación Individual

CertMind definirá medios de identificación y autenticación apropiados, que no podrán ser compartidos y deberán estar habilitados. Dichos medios de autenticación contienen información confidencial que no debe ser revelada o almacenada en lugares que puedan ser accedidos por personas no autorizadas.

5.8. Control y Administración del acceso a la información.

En CertMind se establecen mecanismos de control de acceso lógico para asegurar que los activos de información se mantengan protegidos de una manera consistente con su valor y con los riesgos de pérdida de Integridad, Confidencialidad, Disponibilidad y Privacidad de la información.

El acceso a la información de CertMind deberá ser otorgado sólo a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad. El acceso a los recursos de CertMind debe ser restringido en todos los casos, y se debe dar específicamente a quienes lo requieran debido a sus funciones, con los privilegios apropiados.

5.9. Continuidad del negocio

La información debe estar disponible para su uso autorizado cuando CertMind la requiera en la ejecución de sus tareas regulares. Por lo que se deben diseñar, documentar, implementar y probar periódicamente procedimientos para asegurar una recuperación

razonable y a tiempo de la información crítica de CertMind, sin disminuir los niveles de seguridad establecidos. Esto debe ser independiente tanto del medio tecnológico que utilice CertMind, como de la posibilidad de que la información se dañe, se destruya o no esté disponible por una extensión de tiempo.

CertMind establece medidas de prevención que permiten detectar y mitigar los efectos de ataques contra la seguridad de la información como lo son: el negado de servicio y el ingreso de código no autorizado. Estas medidas estarán fundamentadas en procedimientos y elementos que permitan mantener informado a CertMind de la existencia de estas amenazas, detectar los ataques de manera inmediata y ejecutar las acciones consiguientes.

5.10. Seguridad Lógica.

La seguridad Lógica de CertMind debe basarse por medio de controles apropiados. Estos deben ser consistentes con la información (exámenes, plataformas, materiales, listas de asistencia, bases de datos de clientes, información legal y financiera e informes) que contienen y los derechos mínimos de acceso deben ser otorgados teniendo en cuenta si los sitios de trabajo son permanentes o no.

La información clasificada como confidencial o restringida no se dejará sin control, por lo que CertMind desarrollará un programa que permita prevenir que la información del negocio sea accedida sin autorización.

5.11. Monitoreo de la política de seguridad

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas, analizadas e informadas a la gerencia estratégica y a al área involucrada con la Seguridad de la información de manera inmediata (alertas).

5.12. Uso de los recursos de la información

Los recursos de información de CertMind son exclusivamente para propósitos de la institución y deben ser tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido. Los usuarios que intenten acceder información para la que no tienen un requerimiento autorizado, están violando la presente Política.

Se debe proveer el buen uso de los recursos de información, conservando la intimidad y privacidad de las personas, no se debe presumir privacidad cuando se utilicen recursos de CertMind. Cuando sean utilizados, se deben crear registros de la actividad realizada, que pueden ser revisados con el objetivo de detectar abusos y amenazas. En caso de ser así, se ejecutarán los procedimientos correspondientes acorde con las disposiciones legales aplicables.

CertMind se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente.

Personal seleccionado por CertMind podrá utilizar tecnología de uso restringido como la de monitoreo de red, datos operacionales y eventos en seguridad de la información. Ningún hardware o software no autorizados serán cargados, instalados o activados en los recursos de información, sin previa autorización.