UNIVERSIDAD TECNOLÓGICA NACIONAL

SERVICIO INFORMÁTICO Y PROTECCIÓN DE DATOS PERSONALES

1 - Fundamentos de la Protección de Datos Personales

- Explicación de los conceptos clave de protección de datos personales.
- Introducción a las leyes y regulaciones pertinentes en el ámbito de la protección de datos.

2 - Normativas de Seguridad de la Información para Cumplir con Habeas Data

- Presentación de tres normativas de seguridad de la información relevantes para cumplir con los requisitos de "Habeas Data".
  - **Normativa 1**: Seguridad Física y de Datos en Plataformas Informáticas. Explicación detallada de esta normativa y su importancia en la protección de datos.
  - **Normativa 2**: Sistemas de Control de Acceso Lógicos. Descripción de esta normativa y cómo se relaciona con la protección de datos.
  - **Normativa 3**: Clasificación de los Datos. Análisis de esta normativa y su influencia en el manejo adecuado de datos personales.

3 - Clasificación de la Información

- Explicación de la importancia de la clasificación de la información en la protección de datos personales.
- Descripción detallada de cómo se lleva a cabo la clasificación de la información y sus niveles (público, confidencial, secreto, etc.).

- Ejemplos de cómo la clasificación de la información ayuda a garantizar la seguridad de los datos personales.
- Ejemplos concretos de cómo el servicio puede ayudar en la clasificación y protección de datos.

4 - Beneficios y Ventajas de la Clasificación de la Información

- Enumeración de los beneficios de la clasificación de la información en el contexto de la protección de datos personales.
- Destacar cómo contribuye a la seguridad y cumplimiento legal.

5 - Desafíos y Consideraciones en la Implementación

- Discusión de los desafíos potenciales al implementar la clasificación de la información.
- Recomendaciones para superar estos desafíos.

Conclusión

- Resumen de los puntos clave del informe.

Referencias

- Fuentes y documentos legales utilizados en el informe.

OBJETIVO

En cuanto a los objetivos mínimos que se deben cumplir para la protección de los datos personales son Los siguientes:

- Identificar los datos personales: es importante identificar qué datos personales se están recopilando y almacenando, para poder protegerlos adecuadamente.

- Clasificar los datos: es necesario clasificar los datos personales según su nivel de confidencialidad, para poder aplicar medidas de seguridad adecuadas.

- Implementar medidas de seguridad: se deben implementar medidas de seguridad adecuadas, para proteger los datos personales, como el cifrado de datos, la autenticación de usuarios y la gestión de contraseñas.

- Capacitar al personal: es importante que el personal esté capacitado en cuanto a la protección, de datos personales, para que puedan identificar posibles amenazas y tomar medidas, preventivas.

- Realizar auditorías de seguridad: se deben realizar auditorías de seguridad periódicas para, identificar posibles vulnerabilidades y tomar medidas para corregirlas.

- Cumplir con las normativas: es importante cumplir con las normativas y regulaciones en cuanto, a la protección de datos personales, como la Ley de Protección de Datos Personales.

FUNDAMENTOS DE LA PROTECCIÓN DE DATOS PERSONALES

La protección de datos personales es un tema crítico en la seguridad de la información. Se refiere a la protección de la privacidad y la confidencialidad de la información personal de los individuos.

Los fundamentos de la protección de datos personales incluyen la clasificación de datos, la implementación de medidas de seguridad adecuadas, la capacitación del personal, la realización de auditorías de seguridad y el cumplimiento de las normativas y regulaciones en cuanto a la protección de datos personales.

La clasificación de datos permite identificar la naturaleza y el nivel de sensibilidad de la información, lo que facilita la aplicación de medidas de seguridad proporcionales.

La implementación de medidas de seguridad adecuadas, como el cifrado de datos, el control de accesos y la monitorización de eventos, ayuda a prevenir el acceso no autorizado y garantiza la confidencialidad de los datos personales.

La capacitación del personal es esencial para crear conciencia sobre la importancia de la protección una organización esté al tanto de las mejores prácticas en este campo.

Las auditorías de seguridad permiten evaluar regularmente la efectividad de las medidas de protección de datos y garantizar que todos los miembros de y tomar medidas correctivas cuando sea necesario.

Además, es fundamental cumplir con las normativas y regulaciones en cuanto a la protección de datos personales.

En muchos países, existen leyes específicas, como el RGPD en la Unión Europea, que imponen requisitos estrictos sobre la recopilación, el almacenamiento y el procesamiento de datos personales.

El incumplimiento de estas normativas puede dar lugar a sanciones significativas, por lo que las empresas ,deben asegurarse de cumplir con las obligaciones legales.,

Es importante que las empresas adopten las mejores prácticas para proteger los datos personales y prevenir los ataques informáticos destinados a restringir la disponibilidad y a introducir software Malintencionado.

La integridad de los datos y la protección de datos personales son elementos clave en, la construcción de un entorno seguro y confiable en la era digital. ,

En este informe, exploraremos más a fondo cómo un servicio informático puede desempeñar un papel crucial en el cumplimiento de estas prácticas y normativas, centrándonos en la clasificación de la información y su importancia en la protección de datos personales.

Normativas de Seguridad de la Información para cumplir con Habeas Data

La protección de datos personales es una preocupación crítica en la era digital. Para garantizar la seguridad y confidencialidad de la información personal de los individuos, es fundamental contar con una serie de normativas y medidas de seguridad específicas. En este capítulo, exploraremos tres normativas clave que desempeñan un papel fundamental en la protección de datos personales y en el cumplimiento de la legislación de "Habeas Data". Estas normativas abordan aspectos esenciales de la seguridad de la información:

Normativa 1: Pertenencia de Los Datos

OBJETIVO Y ALCANCE

Asegurar la pertenencia, responsabilidad, uso y custodia de los datos en producción y/o en resguardo, a través de una correcta asignación de roles y responsabilidades.

Todos los datos de los sistemas computarizados en producción o no, residentes en soportes de procesamiento o resguardo, de pertenencia del Estado Provincial y comprendidos en los alcances del Decreto Acuerdo 462/96.

La implementación de estos roles y responsabilidades debe ser:

1. Autorizada por el propietario y asignada a los responsables de los datos.
2. Administrada por el responsable de seguridad de las áreas de servicios de sistemas informáticos de cada organismo.
3. Requerida por los clientes internos y externos de acuerdo a niveles o permisos de acceso.
4. Asistida por la Dirección Provincial de Informática o áreas de servicios informáticos en que ella lo delegue.

La responsabilidad de cumplir con esta norma es de todos los organismos pertenecientes al Estado Provincial comprendidos en el Decreto Acuerdo 462/96.

Máxima autoridad de cada organismo, o persona que lo represente.

Responsables de áreas de servicios informáticos dentro de cada organismo.

Clientes internos y externos de los servicios de sistemas informáticos.

Responsable de seguridad de cada área de servicios de informáticos, en cada organismo.

Auditoría de sistemas informáticos evalúa y verifica el cumplimiento de lo expuesto

Normativa 2: Seguridad de Activos Informáticos

Asegurar una razonable protección y salvaguarda de los activos Informáticos propiedad del Estado Provincial

Todos los datos son propiedad del Estado Provincial

Los recursos informáticos son activos valiosos y estratégicos del Estado Provincial y la información que ellos brindan debe ser administrada para el beneficio del ciudadano y no para el de individuos, organismos o clientes específicos.

Esta administración requiere:

1. Facilitar el acceso a los datos en función del nivel de exposición y revelación de los mismos, de acuerdo al grado de criticidad.
2. Responsabilizar de la disponibilidad, integridad, privacidad y confidencialidad a los organismos citados en el alcance.
3. Custodia de los datos a cargo de las áreas que brindan servicios informáticos en los organismos antes mencionados.
4. Proteger los activos informáticos de amenazas, ya sean accidentales o intencionales.
5. Asegurar medidas que permitan evitar, disuadir, prevenir, detectar y recuperar o corregir las posibles amenazas o sus efectos provenientes de : virus informáticos, hackers, fraudes, especuladores, clientes no autorizados, destrucciones, errores, modificaciones, exposiciones indebidas, omisiones, fallas de

equipos, fallas de software, corte de energía, incendios, inundaciones, terremotos, vientos zonales, alta temperatura, penetración de redes, etc.

6. Asegurar la integridad, exactitud, y salvaguarda de todos los sistemas ya sean desarrollados, mantenidos, procesados en forma propia o por terceros.
7. Asegurar de acuerdo con el grado de criticidad, la confidencialidad de los datos, cualquiera sea el medio en que estén soportados.
8. Atenuar el impacto de accidentes o catástrofes.
9. Asegurar la continuidad del funcionamiento de los sistemas computadorizados en los organismos del Estado Provincial.
10. Cumplir con todas las políticas, normas, procedimientos y estandares de seguridad vigentes, relacionados a los activos informáticos.

RESPONSABLES

Todo el personal, permanente o contratado del Estado Provincial, que interactué de alguna forma, con los servicios y sistemas informáticos.

Auditoría de Sistemas de Información evalúa y verifica el cumplimiento.

Normativa 3: Clasificación de los Datos

La clasificación de los datos es un aspecto fundamental de la seguridad de la información. Exploraremos cómo esta normativa permite identificar la naturaleza y el nivel de sensibilidad de los datos, lo que a su vez facilita la aplicación de medidas de seguridad proporcionales. La clasificación de los datos ayuda a garantizar que se asignen recursos adecuados para proteger la información más crítica.

La Normativa de Clasificación de los Datos tiene como objetivo garantizar que los datos sean clasificados y protegidos según su grado de criticidad. Esto significa que los datos deben manejarse considerando niveles de acceso y exposición definidos. Esta normativa establece los criterios para la clasificación de los datos y su aplicación se detalla en la Norma Operativa 2.21/1. Se aplica a todos los datos de los sistemas computarizados,

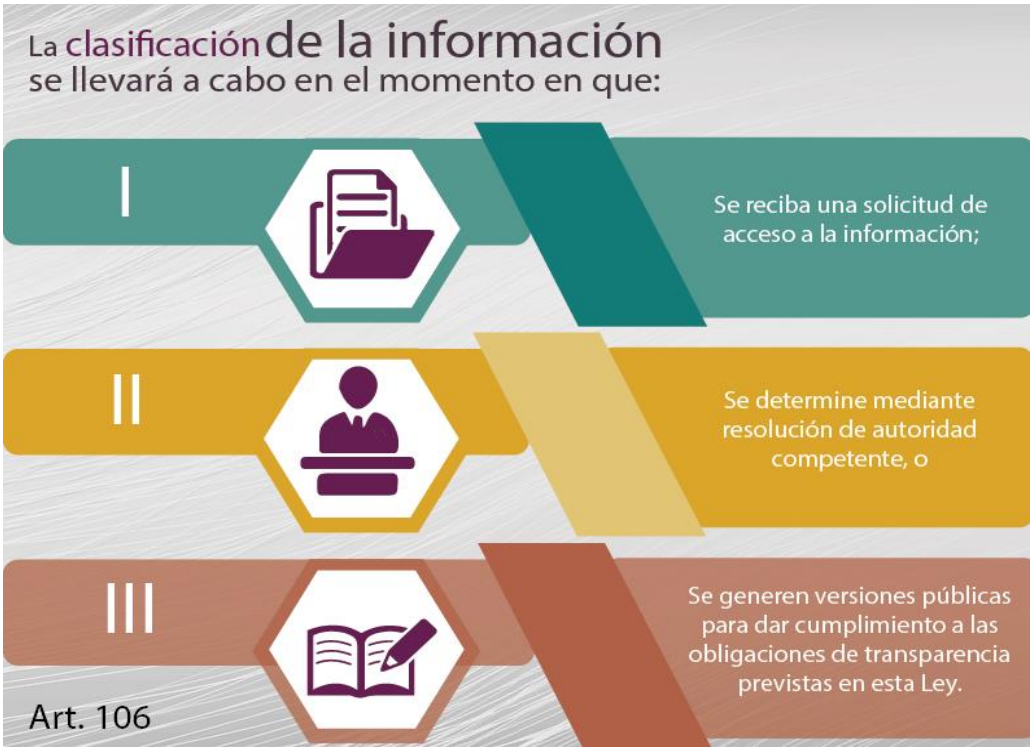
independientemente del soporte en el que estén registrados, en todos los organismos contemplados en el Decreto Acuerdo 462/96 del Gobierno Provincial.

Aspectos Fundamentales para una Empresa: La clasificación de datos es un componente esencial de la seguridad de la información y tiene una gran relevancia para las empresas que manejan datos sensibles, especialmente en el contexto de la protección de datos personales.

CLASIFICACIÓN DE LA INFORMACIÓN

Los aspectos fundamentales de esta normativa incluyen:

1. **Clasificación según Grados de Criticidad:** Los datos deben ser clasificados y manejados considerando grados de criticidad que indican los niveles de acceso y exposición. Se establecen dos categorías principales:
    - **Públicos:** Estos datos se consideran apropiados para su divulgación al público en general. La información pública debe estar disponible a través de publicaciones o documentos autorizados por el Estado Provincial u organismos designados.
    - **Confidenciales:** Los datos confidenciales se distribuyen solo a personas u organismos específicos y deben ser controlados y administrados por el responsable de los datos. Se requieren mecanismos de seguridad tanto físicos como lógicos para gestionar su acceso. La divulgación no autorizada de estos datos podría tener graves implicaciones en la seguridad, aspectos sociales, económicos, estratégicos y oportunidades del Estado Provincial.
2. **Clasificación Basada en el Mayor Grado de Criticidad:** Los datos deben ser clasificados considerando el grado de criticidad más alto que posea cualquier elemento dentro de su estructura. Esto significa que, si un elemento de datos se considera confidencial, toda la información que incluya ese elemento se tratará como confidencial.



Responsables: Los responsables de cumplir con esta normativa son los responsables de los datos, quienes deben clasificar los datos en grados de criticidad, teniendo en cuenta el nivel de exposición al que podrían estar sujetos. Los responsables de Administración de Seguridad son los encargados de implementar las políticas, normas y procedimientos de seguridad relacionados con el acceso a los datos. La Auditoría de Sistemas de Información tiene la responsabilidad de evaluar y verificar el cumplimiento de estas políticas y normativas.

La implementación de esta normativa es esencial para garantizar la protección adecuada de los datos, especialmente aquellos que son confidenciales y críticos para el funcionamiento de la organización. La clasificación de datos facilita la aplicación de medidas de seguridad proporcionales y asegura que se apliquen los controles de acceso adecuados para cada tipo de información. Además, contribuye al cumplimiento de regulaciones de protección de datos y a la gestión de riesgos de seguridad de la información.

EJEMPLOS PARA CADA NORMATIVA

Ejemplos concretos de cómo el servicio puede ayudar en la clasificación y protección de datos.

Normativa 1: Pertenencia de Datos

Ejemplo de Cómo el Servicio Puede Ayudar:

Para cumplimentar el objetivo de la norma, se debe definir los siguientes roles:

1- Propietario del dato: Estado Provincial.
2- Responsable del dato: Máxima autoridad de cada organismo sobre la salvaguarda, integridad, exactitud y uso de los mismos.
3- Custodia del dato: Áreas de servicios informáticos dentro de los organismos centralizados y descentralizados.

4- Utilización del dato: Clientes internos y externos, debidamente autorizados por el responsable del dato.

Normativa 2: Seguridad de Activos de Informaticos

Ejemplo de Cómo el Servicio Puede Ayudar:

Todo el personal, permanente o contratado del Estado Provincial, que interactué de alguna forma, con los servicios y sistemas informáticos. Auditoría de Sistemas de Información evalúa y verifica el cumplimiento.

Debes tener en cuenta que es crucial protegerlos para mantener seguras las claves y la información de los distintos proyectos empresariales o personales. Se defiende ante posibles daños y alteraciones en los datos.

Esta gestión de los activos informáticos permite:

1- Cumplir con las políticas corporativas sobre seguridad y requisitos normativos
2- Mejorar la productividad utilizando la tecnología para solventar las necesidades de los usuarios y empresas
3- Disminuir costes de soportes y licencias eliminando los recursos y licencias que no se aprovechan
4- Restringir los costes de la gestión de recursos informáticos y activos

Ejemplos de activos informáticos:

1- HARDWARE DE INFRAESTRUCTURAS: dispositivos de red, datos, servicios físicos
2- SOFTWARE DE LA EMPRESA: comprende el trabajo llevado a cabo por los informáticos de su empresa
3- LICENCIAS DE SOFTWARE: licencias que su empresa ha pagado para poder usar programas creados por otros
4- DISPOSITIVOS PROPIEDAD DE LA EMPRESA: comprende todos aquellos dispositivos que han sido suministrados por la empresa para su uso, a excepción de los que aportan los propios empleados
5- PRODUCTOS TECNOLÓGICOS: pendrives, impresoras, ordenadores, móviles
6- DATOS DIGITALES DE LAS OPERACIONES: los datos que se almacenan de su empresa digitalmente son muy valiosos, sobre todo los llamados datos operacionales. Incluye la información confidencial en la red
7- EQUIPOS INFORMÁTICOS: poseen acceso a servidores, redes y documentos personales
8- CONTRATOS DE ARRENDAMIENTOS DE INSTALACIONES E INFRAESTRUCTURAS

Normativa 3: Clasificación de los Datos

Ejemplo de Cómo el Servicio Puede Ayudar:

Supongamos que una organización maneja una gran cantidad de datos, algunos de los cuales son confidenciales y otros públicos. Para cumplir con la normativa de clasificación de datos, el servicio de seguridad podría implementar las siguientes medidas:

1. **Etiquetado de Datos:** El servicio podría desarrollar un sistema de etiquetado de datos que clasifique automáticamente la información en función de su contenido y nivel de confidencialidad. Esto facilitaría la identificación y gestión de datos críticos.

2. **Control de Acceso Basado en Clasificación:** Se podría establecer un sistema de control de acceso que garantice que solo los usuarios autorizados tengan acceso a datos clasificados como confidenciales. Esto se lograría mediante la asignación de permisos de acceso específicos.

3. **Encriptación de Datos Sensibles:** Los datos clasificados como confidenciales podrían ser encriptados para protegerlos contra el acceso no autorizado, incluso en caso de una brecha de seguridad.

4. **Auditoría de Acceso a Datos:** Se podría implementar un sistema de auditoría que registre y supervise quién accede a los datos confidenciales y cuándo lo hace. Esto proporcionaría un registro detallado de actividades relacionadas con datos críticos.

5. **Formación y Concienciación:** El servicio podría ofrecer capacitación y concienciación al personal sobre la importancia de la clasificación de datos y las prácticas de seguridad asociadas.

Estos ejemplos ilustran cómo un servicio de seguridad puede desempeñar un papel fundamental en la implementación de las normativas de seguridad, contribuyendo a la clasificación y protección adecuada de los datos en una organización.

BENEFICIOS Y VENTAJAS DE LA CLASIFICACION DE LA INFORMACIÓN

La clasificación de la información en el contexto de la protección de datos personales ofrece una serie de beneficios significativos que contribuyen tanto a la seguridad como al cumplimiento legal. Aquí hay una enumeración de los principales beneficios:

- **Mejora de la Gestión de Riesgos:** La clasificación de datos permite identificar y priorizar los datos más críticos y sensibles. Esto facilita la asignación de recursos y medidas de seguridad adecuadas a los datos de mayor riesgo, reduciendo así la probabilidad de violaciones de seguridad.

- **Protección Personalizada:** Cada categoría de datos puede recibir un nivel específico de protección según su grado de sensibilidad. Esto asegura que los datos personales se protejan de manera proporcional a su importancia y nivel de riesgo.

- **Cumplimiento Legal:** La clasificación de datos ayuda a cumplir con las regulaciones específicas de protección de datos en Argentina, como la Ley de Protección de Datos Personales (Ley 25.326) y su normativa complementaria. Estas regulaciones establecen requisitos rigurosos para el tratamiento de datos personales y requieren que las organizaciones implementen medidas de seguridad adecuadas.

- **Mayor Conciencia de la Sensibilidad de los Datos:** Al clasificar datos, las organizaciones y su personal adquieren una mayor conciencia de la importancia de proteger la privacidad y la confidencialidad de los datos personales. Esto puede llevar a una cultura de seguridad más sólida en la organización.
- **Optimización de Recursos:** La clasificación de datos permite asignar recursos de seguridad de manera más eficiente. Los datos públicos pueden requerir menos protección que los datos confidenciales, lo que ahorra tiempo y recursos.
- **Gestión de Accesos Precisa:** Con la clasificación, es más fácil implementar sistemas de control de acceso que limiten el acceso solo a usuarios autorizados. Esto evita que personal no autorizado acceda a datos sensibles.
- **Facilita la Notificación de Brechas de Seguridad:** En caso de una violación de datos, la clasificación ayuda a determinar qué datos se vieron comprometidos y qué acciones se deben tomar. Esto facilita el proceso de notificación de brechas a las autoridades y a las partes afectadas, en cumplimiento de las regulaciones de notificación.
- **Mayor Confianza del Cliente:** Los clientes y usuarios confían en las organizaciones que demuestran un fuerte compromiso con la protección de sus datos personales. La clasificación y la implementación de medidas de seguridad adecuadas contribuyen a ganar esa confianza.
- **Reducción de Costos Legales y Multas:** Cumplir con las regulaciones de protección de datos a través de la clasificación adecuada puede ayudar a evitar multas y sanciones legales asociadas con incumplimientos de seguridad de datos.
- **Protección de la Reputación:** Evitar violaciones de datos y garantizar la protección de datos personales contribuye a mantener una sólida reputación de la empresa. Las violaciones de seguridad pueden dañar gravemente la imagen de una organización.

La implementación de la clasificación de la información en una organización puede ser una estrategia fundamental para proteger los datos y garantizar el cumplimiento de las regulaciones de privacidad. Sin embargo, también presenta desafíos potenciales que deben abordarse de manera efectiva para lograr una implementación exitosa. Aquí discutiremos algunos de estos desafíos y ofreceremos recomendaciones para superarlos:

DESAFIOS

- **Resistencia al Cambio:** Uno de los principales desafíos es la resistencia al cambio por parte del personal. La clasificación de datos puede requerir nuevos procesos y prácticas, y algunos empleados pueden resistirse a adoptarlos.
- **Complejidad de la Clasificación:** Clasificar datos de manera efectiva puede ser complejo, especialmente en organizaciones con grandes volúmenes de información. Determinar qué datos son confidenciales, cuáles son públicos y cómo gestionarlos puede ser una tarea desafiante.
- **Capacitación y Concienciación:** La capacitación adecuada del personal sobre la importancia de la clasificación de datos y las prácticas de seguridad asociadas puede ser costosa y llevar tiempo. Además, mantener una cultura de seguridad de la información puede requerir esfuerzos continuos de concienciación.

- **Implementación Tecnológica:** La implementación de herramientas tecnológicas para facilitar la clasificación de datos puede ser costosa y requerir integración con sistemas existentes.

Recomendaciones para Superar estos Desafíos:

- **Liderazgo y Comunicación:** El liderazgo comprometido y la comunicación efectiva son clave para superar la resistencia al cambio. Los líderes deben comunicar claramente los beneficios de la clasificación de datos y demostrar su apoyo.
- **Políticas y Procedimientos Claros:** Establecer políticas y procedimientos claros para la clasificación de datos ayuda a guiar a los empleados en el proceso. Deben ser fáciles de entender y seguir.
- **Capacitación Continua:** Proporcionar capacitación continua sobre la clasificación de datos y las prácticas de seguridad de la información. Esto puede incluir ejercicios de concienciación y simulacros de respuesta a incidentes.
- **Herramientas Tecnológicas:** Implementar herramientas tecnológicas, como software de clasificación de datos y soluciones de encriptación, para simplificar el proceso de clasificación y protección de datos.
- **Evaluación y Mejora Continuas:** Regularmente, revise y mejore sus prácticas de clasificación de datos en función del feedback de los empleados y las auditorías de seguridad. Asegúrese de que las políticas y procedimientos se mantengan actualizados.
- **Colaboración Interdepartamental:** Fomente la colaboración entre los departamentos de TI, seguridad de la información, legal y cumplimiento para garantizar una implementación efectiva de la clasificación de datos.
- **Monitorización y Cumplimiento:** Implemente sistemas de monitorización para garantizar el cumplimiento continuo de las políticas de clasificación de datos y tome medidas proactivas en caso de incumplimiento.

CONCLUSIÓN

La protección de datos es el proceso de salvaguardar información importante contra corrupción, filtraciones, pérdida o compromiso de los datos.

La importancia de la protección de datos aumenta a medida que la cantidad de datos creados y almacenados sigue creciendo a un ritmo sin precedentes. También hay poca tolerancia para el tiempo de inactividad que puede hacer que sea imposible acceder a información importante.

En consecuencia, una gran parte de una estrategia de protección de datos es garantizar que los datos se puedan restaurar rápidamente después de cualquier daño o pérdida. Proteger los datos de cualquier compromiso y garantizar la privacidad de los datos son otros componentes clave de la protección de datos.

La pandemia de coronavirus provocó que millones de empleados trabajaran desde casa, lo que resultó en la necesidad de una protección de datos remota. Las empresas deben adaptarse para asegurarse de proteger

los datos dondequiera que estén los empleados, desde un centro de datos central en la oficina hasta las computadoras portátiles en casa.

En esta guía, explore lo que implica la protección de datos, las estrategias y tendencias clave, y los requisitos de cumplimiento para mantenerse al frente de los muchos desafíos de proteger las cargas de trabajo críticas.

Referencias

- NORMATIVAS INTERNAS COMPLETAS - REFERENCIAS.
- LEY 11.723 PROPIEDAD INTELECTUAL.
- LEY DE PROTECCIÓN DE DATOS PERSONALES.
- LA INTEGRIDAD DE LOS DATOS.

Alumno: Quiñonez Nelson Damian Grupo: WorkBots Materia: Legislación