Capacitación Gestión de Seguridad de la información para la empresa CareCloud

UNIVERSIDAD EL BOSQUE

Universidad El Bosque, 2021

Seguridad de la información

Es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad y la integridad de los datos.

Confidencialidad

Es la cualidad de la información que indica que no puede ser divulgada a personas o sistemas no autorizados.

Se trata básicamente de la propiedad por la que esa información solo resultará accesible con la debida y comprobada autorización.

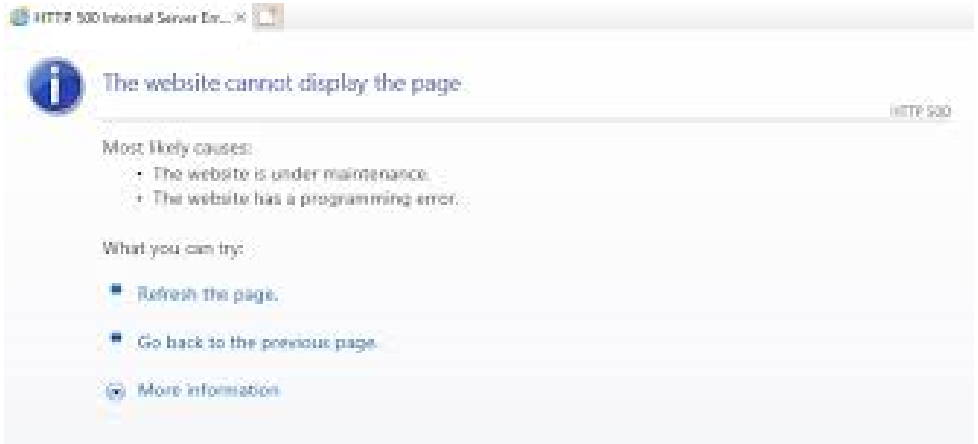
¿Cómo se pierde la confidencialidad?

Cuando no se hace un correcto uso según lo establecido en las políticas de seguridad de la información como por ejemplo:

- Compartiendo las contraseñas.
- No cerrando la sesión de aplicativos que no están en uso.
- Dejando desbloqueado el equipo.
- Descuidando los documentos físicos.

Disponibilidad

Es aquella información o servicio al que podemos acceder cuando lo necesitamos.



Prevenir fallas o intermitencias en los recursos informáticos con el fin de mantener la disponibilidad de la información o los servicios

Integridad

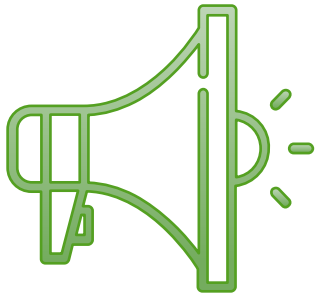
Hace referencia a la cualidad de la información de ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.

La integridad de la información se pierde cuando **es modificada** o cuando parte de ella **se elimina**.

- Modificada
- Alterada
- Eliminada

La información corporativa debe estar clasificada en información pública, de uso interno y confidencial. Los documentos y registros utilizados por la organización deben tener la etiqueta que identifique la clasificación correspondiente a la información que se incluya.

Clasificación de la información



Uso Interno | **Público**

CONFIDENCIAL

Información que es sensible para el negocio o para un individuo al cual se le afecten sus datos personales.

Su divulgación tiene el potencial de interrumpir o afectar total o parcialmente las actividades, operaciones y/o seguridad de la Organización y sus partes interesadas, o causar un daño severo a su estabilidad, a su imagen corporativa o su continuidad.

En atención al impacto que puede ocasionar su divulgación o adulteración se dispone que esta información deberá ser protegida, tanto en su almacenamiento como en su transmisión, de manera tal que se asegure que sólo tenga acceso a ella el personal debidamente autorizado.

USO INTERNO

Es la información necesaria para llevar a cabo las actividades y operaciones de la Organización y que debe ser mantenida dentro de la Organización.

El acceso debe ser determinado por el dueño de la información y debe ser autorizado a los grupos de usuarios según las tareas que realizan. Esta información es divulgada internamente sin restricciones y sólo puede ser divulgada a un tercero, si previamente existe una autorización para su entrega.

PÚBLICO

Es la información que puede ser conocida por personas internas o externas sin ningún perjuicio para las actividades, operaciones y/o seguridad de la Organización y sus partes interesadas.

Esta información ha sido aprobada para la difusión pública. Quien entrega la autorización es el dueño de la información. Se considera Información de uso público a toda aquella, que además de compartirse con la compañía podría ser de uso de los clientes o proveedores, ejemplo: folletos e información expuesta en página Web

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

Es un sistema que nos permite establecer, implementar, monitorear, verificar, mantener y mejorar la seguridad de la información en nuestra compañía según lo establecido en el estándar ISO 27001:2013.

Así mismo, todo el personal de la empresa está inmerso para llevar a cabo las mejores prácticas y hacer el uso adecuado de la información tratada dentro de la misma.

Alcance del SGSI

Esta política debe ser aplicada y cumplida por todos los colaboradores, proveedores de servicio, socios de negocio que usan, mantienen o son responsables de activos de información, así como también debe ser aplicada y cumplida por cada sistema de información y aplicación de la empresa CareCloud. Cualquier excepción a esta norma será permitida solamente cuando sean aprobadas previamente por escrito por la gerencia general.

Roles y Responsabilidades

Oficial de seguridad de la información

Es el encargado de implementar, coordinar, elaborar y dirigir la revisión periódica de esta política y los controles que ella comprende

Junta Directiva

Certificar que los controles abordados en esta política se ejecuten y cumplan, identificar cómo se manejan los no cumplimientos, promover la difusión y sensibilización de las materias abordadas en este documento, revisar y aprobar está política, así como los cambios o planes de mejora que se realicen sobre la misma.

Roles y Responsabilidades

Jefe Departamento de TI y Comunicaciones

Evaluar e implementar las propuestas de mejora establecidas por la Junta Directiva. Además, debe revisar periódicamente la política detectando y proponiendo mejoras.

Jefe Recursos Humanos

Notificar a todo el personal que se vincule con la empresa de los compromisos para el cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos y procedimientos que surjan del Sistema de Gestión de Seguridad de la Información.

Personal/Usuarios

Cumplir en su totalidad con las disposiciones y requerimientos establecidos en la presente política. Cada usuario de la información, equipos informáticos y de los servicios de red deberá velar por la correcta implementación de las normas de seguridad de la información promovidas dentro de sus áreas de responsabilidad, así como del cumplimiento por parte de su equipo de trabajo.

Gestión de activos

Cada área debe velar por mantener actualizado el inventario de los activos físicos y lógicos de la organización, garantizando las características del inventario, donde se incorpore la clasificación, valorización, ubicación y acceso de la información.

Las áreas deben garantizar mediante un formato establecido por el área de seguridad de la información el tratamiento y transporte que se requiera de los activos físicos y lógicos

TIPO DE ACTIVO	DESCRIPCIÓN
Información Electrónica	Cualquier tipo de información contenida en un medio digital, bien sean bases de datos, archivos de datos, documentos, contratos, manuales, procedimientos, instructivos, etc.
Información Física	Cualquier tipo de información contenida en un medio físico, bien sean contratos, manuales, procedimientos, instructivos, acuerdos, propuestas, etc.
Hardware	Cualquier componente físico que sea necesario para efectuar o complementar operaciones sobre activos de información, como equipo de comunicación, equipo de cómputo, medios removibles, etc..
Software	Todo sistema de información, sistema operativo, aplicación, utilitario o herramienta adquirida o desarrollada al interior de la organización, que realice operaciones, transacciones y que requiera la interacción de uno o más activos de información para efectuar sus tareas.
Persona	Toda persona, proveedor o cliente que realice funciones críticas para la organización, cuya ausencia o incumplimiento de tales funciones puede desencadenar un alto impacto para la misma.
Servicio	Es el conjunto de actividades desarrolladas por una persona, proceso o sistema, que busca responder a las necesidades de un cliente.
Infraestructura	Todo el conjunto de elementos o servicios que están considerados como necesarios para que una organización pueda funcionar o bien para que una actividad se desarrolle efectivamente.

Tipos de activos de información

Recomendaciones

- Las partes interesadas de la organización tienen la responsabilidad de reportar de inmediato cualquier evento como robo, pérdida o divulgación no autorizada de información de propiedad de la empresa a Seguridad de la Información.
- Los usuarios deben evitar abrir archivos adjuntos de correo electrónico recibidos de remitentes desconocidos, que pueden contener código malicioso.
- Los usuarios que cuentan con acceso al servidores de archivos (On premise o en la nube), deben guardar allí la información que se considere importante para el proceso y para la organización, la cual se respalda para garantizar su disponibilidad en caso de presentarse un daño en el computador.

Recomendaciones

- Los usuarios solo tendrán acceso a los datos y los recursos tecnológicos necesarios para el desempeño de sus actividades laborales, serán responsables disciplinaria, administrativa y legalmente por la divulgación no autorizada de información corporativa.
- Los usuarios deben evitar abrir archivos adjuntos de correo electrónico recibidos de remitentes desconocidos, que pueden contener código malicioso.
- Todo usuario de la organización debe poseer una única cuenta en cada uno de los sistemas y aplicaciones de información que tenga acceso autorizado.
- Los colaboradores nunca deben anotar las contraseñas de acceso en lugares visibles o de baja seguridad.

Recomendaciones

- Cada usuario es responsable del uso responsable de su cuenta y toda actividad que se realice con ella.
- El inventario de activos de información debe estar identificado por cada área con apoyo de seguridad de la información para tenerla actualizada y disponible.
- Por razones de seguridad y mantenimiento de la red, las personas autorizadas por la empresa pueden realizar el monitoreo y la auditoria de equipos, sistemas y el tráfico de red en cualquier momento.
- El uso y/o instalación de software sin autorización, está prohibido por la organización. Solo las personas de Soporte Técnico están autorizadas para instalar software en los equipos informáticos de la compañía con previa autorizar de parte del área de seguridad de la información.