



Unidad que genera el documento: Especialización Seguridad en Redes Telemáticas

Nombre del documento: Capacitación SGSI – Empresa CareCloud

Fecha: 02-11-2021

Versión: 1

Objetivo: El objetivo es socializar a la empresa CareCloud y cada uno de sus empleados, los conceptos generales y las responsabilidades según el Sistema de Gestión de Seguridad de la Información.

Cuestionario

1. ¿Cuáles son los principios de Seguridad de la Información?
 - a. Integridad, confidencialidad y Disponibilidad
 - b. Integridad, continuidad y Disponibilidad
 - c. Integridad, continuidad y Oportunidad
 - d. Ninguna de las anteriores

2. ¿Quién es el encargado de implementar, coordinar, elaborar y dirigir la revisión periódica de esta política y los controles que ella comprende?
 - a. Junta Directiva
 - b. Jefe de departamento de TI y Comunicaciones
 - c. Oficial de Seguridad de la Información
 - d. Todas las anteriores

3. ¿Quién puede acceder, usar y compartir la información corporativa?
 - a. Los Gerentes y Subgerentes
 - b. Los vicepresidentes y jefes
 - c. Solo el personal expresamente autorizado para el cumplimiento de sus funciones laborales
 - d. Todos los Anteriores

4. ¿Quién debe cumplir lo establecido por el SGSI?
 - a. Socios del negocio y Junta Directiva
 - b. Por cada persona que haga uso, mantenga o sea responsable de activos de información
 - c. Gerencia General
 - d. Colaboradores y Proveedores.

5. ¿En qué categorías debe clasificarse la información?
- Pública, Privada y Confidencial
 - Confidencial, Pública y Secreta
 - Pública, Uso interno y Uso Externo
 - Pública, Uso interno y Confidencial**
6. Para la gestión de activos, ¿Qué activos deben tenerse en cuenta al realizar el inventario de estos por cada área?
- Físicos
 - Administrativos
 - Lógicos
 - a y c**
7. La integridad de la información se refiere a:
- La cualidad de la información que indica que no puede ser divulgada a personas o sistemas no autorizados.
 - Toda información o servicio al que podemos acceder cuando lo necesitamos.
 - La cualidad de la información de ser correcta y no haber sido modificada.**
 - Proteger la información y resguardarla en ambientes seguros.
8. ¿En qué momento los usuarios deben bloquear o cerrar la sesión en los computadores?
- Cuando se haya finalizado la jornada laboral.
 - cada vez que se ausente del puesto de trabajo
 - a y b**
 - Nunca.
9. ¿Cuándo deben retirarse los documentos impresos o digitalizados de los dispositivos usados para dicho fin?
- A más tardar una hora después de ser impreso o digitalizado.
 - A más tardar dos horas después de ser impreso o digitalizado.
 - Estos deben retirarse inmediatamente.**
 - Cuando el funcionario lo considere pertinente.
10. Se establece, implementa, mantiene y mejora continuamente el Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con los requisitos del estándar ISO 27001:2013.
- VERDADERO**
 - FALSO

11. La confidencialidad de la información se refiere a:
- a. Toda información o servicio al que podemos acceder cuando lo necesitamos.
 - b. La cualidad de la información que indica que no puede ser divulgada a personas o sistemas no autorizados.
 - c. La cualidad de la información de ser correcta y no haber sido modificada.
 - d. Todos los anteriores.
12. El personal o los usuarios están exentos de cumplir con algunas de las políticas establecidas por el SGSI por desconocimiento parcial o total del mismo.
- a. Verdadero
 - b. Falso
13. ¿A quién se le debe reportar cualquier evento de robo, pérdida o divulgación no autorizada de información?
- a. Al jefe inmediato.
 - b. A la mesa de servicio.
 - c. A soporte tecnico.
 - d. A Seguridad de la Información.

[Redacted]	
Ivonne Tatiana Carreño B	Sebastian Mendoza
Mateo José Montañez Usme	