**Seguridad Informática - Empresa tipo 2**

**Grupo 2:**

Daniel Cuellar

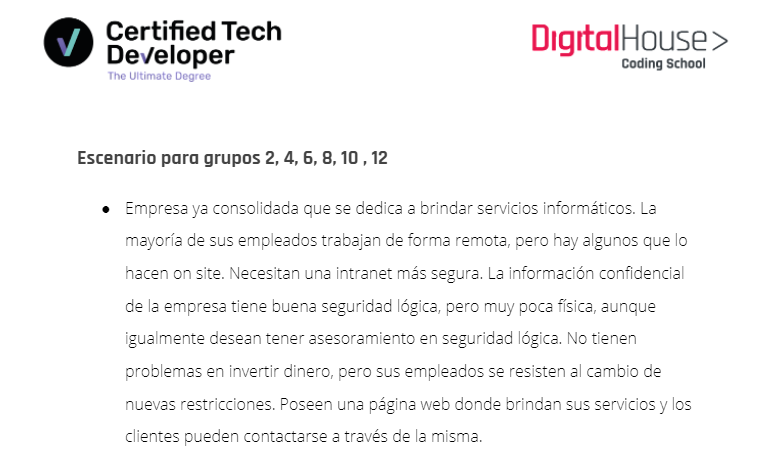
Delfina Molter

Carla Nieto

Coty Javega

Fernando Escobar

**PARTE 1: PLAN DE SEGURIDAD PROPUESTO**



* Seguridad Física:
  + Instalar UPS, para asegurar los datos ante cortes energéticos.
  + Contratar un cloud-service de backup con un período definido.
  + Comprar e instalar sistemas redundantes.
  + Reforzar infraestructura añadiendo: pararrayos, seguridad ante incendios (detectores de humo,extintores, etc).
  + Control de acceso a las terminales físicas por parte de personas externas a la organización o personal con accesos restringidos (instalación de alarmas contra intrusos).
  + Disponer y organizar los equipos con el fin de evitar daños por manipulación indebida.
  + Evitar el ingreso de unidades flash externas (USB, discos duros externos, etc.) a las corporativas (disminuir su uso, fomentar el uso de herramientas cloud).
* Seguridad Lógica:
  + VPN, para permitir el acceso seguro de los trabajadores remotos.
  + Cifrado de datos: Usuario/contraseña para el acceso a la página.
  + Instalar antivirus y firewalls.
* Controles de Medidas de seguridad y vulnerabilidades:
  + Auditorías periódicas informativas con revisión de código para detectar brechas de seguridad.
  + Verificación de realización copias de seguridad.
  + Gestión de permisos (principio del mínimo privilegio).

**AUDITORIA REALIZADA POR EL GRUPO 3:**

Al validar el plan de seguridad propuesta se encuentra que está bien estructurado desde todas las seguridades y controles establecidos, garantizando el control de los ataques tanto para los empleados que asisten a la oficina como para los que trabajan de forma remota.

**PARTE 2: Auditoria plan grupo 3 realizada por el grupo 2**

1. Un análisis de la situación actual de cada empresa que se les haya asignado.

**Pro:**

El personal está trabajando on site y está dispuesto a recibir capacitaciones. Venta online.

**Contra:**

No realizan copia de seguridad de la información. Todos tienen acceso a la información de la empresa. No se tiene clara la seguridad en la página WEB para los usuarios al momento de comprar.

Comentarios grupo 2: capacidad financiera acotada.

2. Para cada escenario planteado, crear un plan de seguridad

3. Este plan debe ser de 6 pasos e incluir: seguridad lógica, física, pasiva, activa y

controles de medida de seguridad y de vulnerabilidades que podrían explotar

los atacantes.

**Seguridad lógica**: Colocar control de acceso a los usuarios para que no todos tengan acceso al total de la información sino depende del rol y área. Colocar un firewall para la página web para asegurar las compras online.

Comentarios grupo 2: Uso de herramientas como Kaspersky para la gestión de contraseñas y seguridad en la web (compras, accesos malintencionados)

**Seguridad Física**: Crear un respaldo de datos / sistemas redundantes.

Comentarios grupo 2: los sistemas redundantes son costosos.

**Seguridad Pasiva:** Tener partición de disco duro en cada computador de los empleados para poder recuperar en caso de algún daño o ataque, y generar backup en la nube constantemente.

Comentarios grupo 2: Depende del volumen de información, manejar backup en físico puede ser más costoso e inclusive tener más riesgos de perder la información que un buen gestor en la nube.

Se sugiere escanear periódicamente los equipos en busca de malware.

**Seguridad Activa:** Que los empleados tengan contraseñas seguras para acceder a la red de la empresa, y que tengan instalados en sus computadores antivirus.

Comentarios grupo 2: adicional prohibir el acceso a páginas web o links desconocidos a través de la VPN.

**Controles de medida de Seguridad:** Generar controles proactivos de tipo preventivas, esto con el fin de bloquear algún ataque y generar la mayor seguridad.

Comentarios grupo 2: ejemplo: utilización de contraseñas robustas.

Se adicionan medidas reactivas de costo bajo como control de versiones para restauración en caso de ataque.

**Vulnerabilidades:** Delimitar quién puede y debe acceder a la información confidencial. Probar que las copias de seguridad realizadas funcionen.

Comentarios grupo 2: Se debe realizar un control constante sobre los privilegios de seguridad para retirar y asignar los accesos necesarios cuando una persona ingresa o sale de la empresa, y cuando es contratada o retirada de sus funciones.