

Integrantes:

Jorge Araya Torres,

Gerardo Espinoza,

Andrey Carranza,

Jose Pablo Bolaños

LISTA DE CHEQUEO DE REVISIÓN ESTRUCTURA ORGANIZACIONAL

| Documento / Aspecto a Revisar |  | AUDITOR ASIGNADO | Observaciones |
|--|---|--------------------------|---------------|
| 1. Solicitud de la política del manejo de información de carácter sensible | | | |
| a) Verificar la existencia de mecanismos utilizados para la encriptación de información sensible |  | Gerardo Espinoza Vargas | |
| b) Verificar la utilización de perfiles de VPN para cada uno de los empleados del área de tecnologías de información |  | Jose Pablo Bolaños Calvo | |
| c) Verificar que los empleados ingresen a las reuniones desde su respectivo correo empresarial. |  | Jorge Araya Torres | |
| 2. Solicitar la política para las llamadas telefónicas de TI |  | Andrey Carranza Pérez | |





Integrantes:

Jorge Araya Torres,

Gerardo Espinoza,

Andrey Carranza,

Jose Pablo Bolaños

| Documento / Aspecto a Revisar |  | AUDITOR ASIGNADO | Observaciones |
|---|---|--------------------------|---------------|
| a) Verificar las preguntas que se deben realizar antes de brindar cualquier tipo de información | | | |
| 3. Solicitar la política para el uso correcto de la documentación sensible | | | |
| a) Investigar qué normas existen para el manejo de la documentación en los escritorios. |  | Jorge Araya Torres | |
| b) Verificar las sanciones aplicadas al incumplimiento de alguna de estas políticas. |  | Jose Pablo Bolaños Calvo | |
| 4. Solicitar la política de los sistemas de seguridad de las puertas de acceso restringido. |  | Andrey Carranza Pérez | |
| 5. Verificar la seguridad del espacio en áreas comunes | | | |





Integrantes:

Jorge Araya Torres,

Gerardo Espinoza,

Andrey Carranza,

Jose Pablo Bolaños

| Documento / Aspecto a Revisar |  | AUDITOR ASIGNADO | Observaciones |
|--|---|-------------------------|---|
| a) Solicitar reporte de personas que pueden acceder al área en concreto |  | Gerardo Espinoza Vargas | Se analiza el entorno y personas habituales en el área para detectar posibles riesgos de filtrado de información |
| 6. Reporte de personas que acceden a los equipos | | | |
| a) Verificar que el espacio donde queda el dispositivo sea seguro |  | Jorge Araya Torres | Se verifica si el espacio donde se mantiene usualmente el equipo es seguro y si se tiene la práctica de apagar el mismo, esto por motivos de seguridad. |
| b) Comprobar que el equipo se deje en un estado de suspensión o se encuentre apagado al momento de alejarnos del dispositivo |  | Andrey Carranza Pérez | |
| 7. Analizar que la conexión de red sea segura | | | |

Integrantes:

Jorge Araya Torres,

Gerardo Espinoza,

Andrey Carranza,

Jose Pablo Bolaños

| Documento / Aspecto a Revisar |  | AUDITOR ASIGNADO | Observaciones |
|--|---|--------------------------|---|
| a) Examinar que las redes de la empresa cumplan los estándares de seguridad de Wi-fi |  | Gerardo Espinoza Vargas | Se revisará que la empresa cumpla con estándares básicos de seguridad de red como wpa y mediante algunas pruebas se verificará si se filtra información sensible en el tráfico de la red. |
| b) Ejecutar chequeos periódicos para revisar si la información se filtra o se encuentra debidamente protegida. |  | Gerardo Espinoza Vargas | |
| 8. Revisar los backups de la información sensible | | | Solicitar el estado de las copias de seguridad junto al dispositivo en el que se está almacenando la información, así como también los usuarios que desempeñan las funciones de backups. |
| a) Verificar el estado de las copias de seguridad, y chequear los dispositivos externos donde se almacenan los mismos. |  | Jose Pablo Bolaños Calvo | |
| b) Analizar los perfiles de los empleados capaces de realizar los backups para verificar que cumplan |  | Jose Pablo Bolaños Calvo | |





Integrantes:

Jorge Araya Torres,

Gerardo Espinoza,

Andrey Carranza,

Jose Pablo Bolaños

| Documento / Aspecto a Revisar |  | AUDITOR ASIGNADO | Observaciones |
|---|---|-------------------------|---|
| con los requisitos para el puesto. | | | |
| 9. Revisar los horarios de cierre de zonas restringidas que poseen información vital para la empresa |  | Jorge Araya Torres | Solicitar los horarios en los que cierran las zonas restringidas de dicha empresa y solicitar información de dicho personal de seguridad de la empresa. |
| a) Disponer de un guarda de seguridad o persona encargada de monitorear el acceso a estas zonas. |  | Jorge Araya Torres | |
| 10. Clasificar información por categorías | | Andrey Carranza | Solicitar y analizar el tipo de información para administrar y clasificar en categorías. |
| a) Revisar el tipo de información para ser clasificada y brindarle el tipo de seguridad que requiere de acuerdo con la necesidad de este. |  | Gerardo Espinoza Vargas | |



Integrantes:

Jorge Araya Torres,


Gerardo Espinoza,

Andrey Carranza,

Jose Pablo Bolaños

| Documento / Aspecto a Revisar |  | AUDITOR ASIGNADO | Observaciones |
|--|---|--------------------------|---------------|
| b) Verificar el tipo de seguridad que se va a brindar por categoría. |  | Jose Pablo Bolaños Calvo | |

Hallazgos

| | | | |
|--|----|---------|--|
| Verificar la existencia de mecanismos utilizados para la encriptación de información sensible | | | |
| 1. Cumple con el requerimiento establecido | | | |
| Observación de la Administración | | | |
| Existe una norma que respalda el proceso de encriptación de información sensible, de igual forma se puede evidenciar este proceso de encriptación en los dispositivos de almacenamiento externo. | | | |
| Aceptación | | | |
| Si  | No | Parcial | |

| | | | |
|---|--|--|--|
| Verificar la utilización de perfiles de VPN para cada uno de los empleados del área de tecnologías de información | | | |
| 2. Cumple parcialmente con el requerimiento establecido | | | |
| Observación de la Administración | | | |
| Se realiza una asignación de ip que se guarda para cada máquina de las respectivas áreas de la empresa, pero no existe evidencia de la utilización de alguna VPN. | | | |


Integrantes:


Jorge Araya Torres,


Gerardo Espinoza,


Andrey Carranza,

Jose Pablo Bolaños

| | | | |
|------------|----|---------|---|
| Aceptación | | | |
| Si | No | Parcial |  |

| | | | |
|--|---|----|---------|
| Verificar que los empleados ingresen a las reuniones desde su respectivo correo empresarial. | | | |
| 3. Cumple con el requerimiento establecido | | | |
| Observación de la Administración | | | |
| Se evidencia el uso de correos empresariales para estas reuniones y procesos en general. | | | |
| Aceptación | | | |
| Si |  | No | Parcial |

| | | | |
|---|----|---|---------|
| Verificar las preguntas que se deben realizar antes de brindar cualquier tipo de información | | | |
| 4. No cumple el requerimiento | | | |
| Observación de la Administración | | | |
| No se evidencia en el documento de políticas de seguridad de la información algún punto que trate sobre llamadas telefónicas. | | | |
| Aceptación | | | |
| Si | No |  | Parcial |

| | | | |
|--|----|---|---------|
| Investigar qué normas existen para el manejo de la documentación en los escritorios. | | | |
| 5. No cumple el requerimiento | | | |
| Observación de la Administración | | | |
| No existe evidencia del manejo de estos documentos. | | | |
| Aceptación | | | |
| Si | No |  | Parcial |


Integrantes:


Jorge Araya Torres,


Gerardo Espinoza,

Andrey Carranza,

Jose Pablo Bolaños


| | | | |
|--|----|---|---------|
| Verificar las sanciones aplicadas al incumplimiento de alguna de estas políticas. | | | |
| 6. No cumple el requerimiento | | | |
| Observación de la Administración | | | |
| Existe la restricción y manejo del acceso a las áreas con información de sensible, pero no se aborda el tema de las sanciones. | | | |
| Aceptación | | | |
| Si | No |  | Parcial |


| | | | |
|--|----|---------|---|
| Solicitar la política de los sistemas de seguridad de las puertas de acceso restringido. | | | |
| 7. No cumple el requerimiento | | | |
| Observación de la Administración | | | |
| Existen controles de acceso manuales, pero no existe un control electrónico. | | | |
| Aceptación | | | |
| Si | No | Parcial |  |


| | | | |
|--|----|---|---------|
| Solicitar reporte de personas que pueden acceder al área en concreto. | | | |
| 8. No cumple el requerimiento | | | |
| Observación de la Administración | | | |
| No se evidencia la seguridad en el acceso en áreas comunes, solamente existe un control en áreas que contengan información sensible. | | | |
| Aceptación | | | |
| Si | No |  | Parcial |

Integrantes:

Jorge Araya Torres,
Gerardo Espinoza,
Andrey Carranza,
Jose Pablo Bolaños

| | | | |
|--|---|----|---------|
| Verificar que el espacio donde queda el dispositivo sea seguro | | | |
| 9. Cumple el requerimiento | | | |
| Observación de la Administración | | | |
| Se evidencia un control para la responsabilidad de la tenencia de los dispositivos tecnológicos hacia los empleados. | | | |
| Aceptación | | | |
| Si |  | No | Parcial |

| | | | |
|---|----|---|---------|
| Comprobar que el equipo se deje en un estado de suspensión o se encuentre apagado al momento de alejarnos del dispositivo | | | |
| 10. No cumple el requerimiento | | | |
| Observación de la Administración | | | |
| No existe una evidencia del estado en el que quedan los dispositivos luego de su uso. | | | |
| Aceptación | | | |
| Si | No |  | Parcial |

| | | | |
|---|----|---|---------|
| Examinar que las redes de la empresa cumplan los estándares de seguridad de Wi-Fi. | | | |
| 11. No cumple el requerimiento | | | |
| Observación de la Administración | | | |
| No existe una evidencia de que se utilice algún tipo de estándar de red para la conexión a Wi-Fi. | | | |
| Aceptación | | | |
| Si | No |  | Parcial |


Integrantes:


Jorge Araya Torres,


Gerardo Espinoza,

Andrey Carranza,

Jose Pablo Bolaños


| | | | |
|---|---|----|---------|
| Ejecutar chequeos periódicos para revisar si la información se filtra o se encuentra debidamente protegida. | | | |
| 12. Si se cumple el requerimiento | | | |
| Observación de la Administración | | | |
| Como mínimo cada mes, se realizar un chequeo para verificar la integridad de la información. | | | |
| Aceptación | | | |
| Si |  | No | Parcial |


| | | | |
|--|----|---|---------|
| Verificar el estado de las copias de seguridad, y chequear los dispositivos externos donde se almacenan los mismos. | | | |
| 13. No cumple el requerimiento | | | |
| Observación de la Administración | | | |
| No hay documento que indique la verificación de las copias de seguridad, así como el chequeo de los dispositivos que almacenan esta información. | | | |
| Aceptación | | | |
| Si | No |  | Parcial |


| | | | |
|---|---|----|---------|
| Analizar los perfiles de los empleados capaces de realizar los backups para verificar que cumplan. | | | |
| 14. Se cumple el requerimiento | | | |
| Observación de la Administración | | | |
| Existe un documento que respalda el análisis de los perfiles con el permiso de realizar estas acciones de backup. | | | |
| Aceptación | | | |
| Si |  | No | Parcial |

Integrantes:

Jorge Araya Torres,
Gerardo Espinoza,
Andrey Carranza,
Jose Pablo Bolaños

| | | | |
|--|----|---|---------|
| Revisar los horarios de cierre de zonas restringidas que poseen información vital para la empresa. | | | |
| 15. No cumple el requerimiento | | | |
| Observación de la Administración | | | |
| No se dispone de los horarios para el cierre de zonas restringidas. | | | |
| Aceptación | | | |
| Si | No |  | Parcial |

| | | | |
|--|---|----|---------|
| Disponer de un guarda de seguridad o persona encargada de monitorear el acceso a estas zonas. | | | |
| 16. Se cumple el requerimiento | | | |
| Observación de la Administración | | | |
| Existe un control de acceso físico, a cargo del jefe de la unidad administrativa encargada de realizar el control. | | | |
| Aceptación | | | |
| Si |  | No | Parcial |

| | | | |
|--|---|----|---------|
| Revisar el tipo de información para ser clasificada y brindarle el tipo de seguridad que requiere de acuerdo con la necesidad de este. | | | |
| 17. Se cumple el requerimiento | | | |
| Observación de la Administración | | | |
| Existe una política para cada tipo de información clasificada que se requiere administrar dentro de la empresa. Como por ejemplo políticas para administrar la información de base de datos, políticas para los backups, políticas para administrar las redes y demás áreas. | | | |
| Aceptación | | | |
| Si |  | No | Parcial |


Integrantes:

Jorge Araya Torres,

Gerardo Espinoza,

Andrey Carranza,

Jose Pablo Bolaños

| | | | |
|---|---|----|---------|
| Verificar el tipo de seguridad que se va a brindar por categoría. | | | |
| 18. Se cumple el requerimiento | | | |
| Observación de la Administración | | | |
| Se evidencia mediante un documento, donde se explica la forma de administrar los permisos de las personas que dispondrán del acceso a la información. | | | |
| Aceptación | | | |
| Si |  | No | Parcial |