CORREDOR EMPRESARIAL S.A

Seguridad de la Información

¿Por qué de la Seguridad de la Información?

Porque protege la confidencialidad, integridad y disponibilidad de la información, asegurando que solo personas autorizadas tengan acceso y que los datos estén seguros y accesibles cuando se necesiten.

- Acceso, modificación y eliminación no autorizada
- Fuga de información
- Indisponibilidad del servicio
- Código malicioso
- Espionaje
- Desastres naturales y/o provocados

Confidencialidad

Garantizar que la información únicamente sea accedida por las personas autorizadas

Integridad

Garantizar que la información sea exacta, completa y no sea alterada

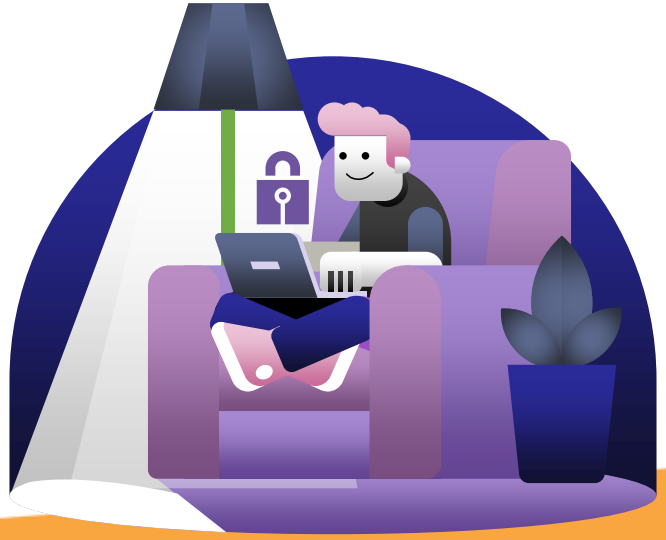
Disponibilidad

Mantener disponible y accesible la información de la organización

Dispositivos Móviles, Teletrabajo y Trabajo en Casa

- Contar con usuario y contraseña y velar por que la información almacenada en el equipo se encuentre debidamente cifrada o protegida.
- Los dispositivos móviles no corporativos se considerarán como inseguros por defecto y no podrán conectarse a ninguna red corporativa, ya sea esta cableada o inalámbrica, deberán emplear una red separada establecida para sus efectos.
- Evitar dejar el equipo en lugares no seguros.
- Cuando termine la relación contractual con Corredor Empresarial S.A., devolver todos los activos (componentes software, documentos corporativos y equipos prestados) de la organización que tengan en su posesión y estén relacionados con su puesto de trabajo.

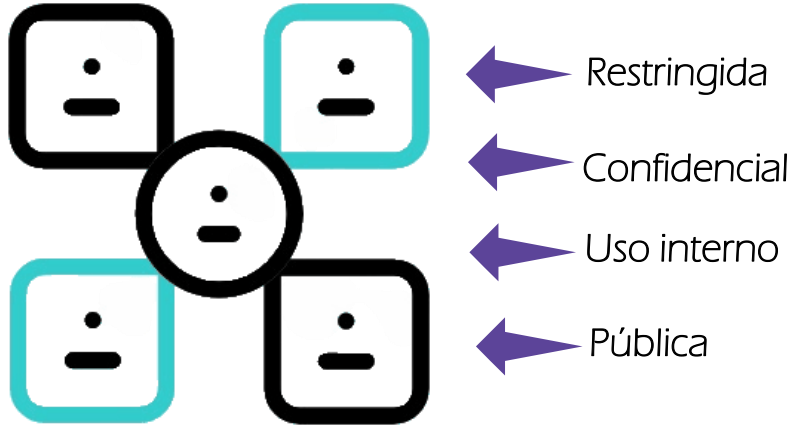
- Conectarse la red corporativa a través de una VPN para una conexión segura.
- Garantizar que el dispositivo móvil esté protegido con el software de protección antimalware y firewall y permitir sus actualizaciones.
- Evitar conectarse desde redes de internet públicas poco seguras (Parques, aeropuertos, etc).
- Bloquear sesión al ausentarse del equipo.
- Informar a las áreas de Tecnología y Seguridad de la información sobre cualquier incidente que pueda comprometer la seguridad de la información.



Manejo de Activos de Información

- Se consideran “Activos de Información”, a todos los elementos que una organización posee para el tratamiento de la información (hardware, software, impresoras, audífonos, etc.) propia de los procesos y sus labores para ejercer su objeto de negocio.

- La aplicación de la **clasificación o etiquetado** de la información debe realizarse por el líder de proceso propietario del activo, quien será el responsable de mantenerla actualizada a lo largo de su ciclo de vida.



Controles Criptográficos

La información Restringida o Confidencial se debe proteger con mecanismos de cifrado apropiados, cuando se procese, almacene o transmita en:

- Información contenida en medios de almacenamiento (USB, Discos, CDs, DVD´s, Cintas, entre otros).
- Copias de Respaldo.
- Información propia o bajo custodia de la compañía transmitida de manera interna o externa, a través de cualquier medio de comunicación o aplicación.
- Información que se tenga almacenada en los centros de procesamiento de datos (datacenter, proveedores, cloud).

Control de Accesos

- Tener procedimientos para acceso físico y de videovigilancia a directivos, empleados, visitantes, contratistas y proveedores a las instalaciones en coordinación con la Gerencia Administrativa, Seguridad de la información y el área de Tecnología e Infraestructura.

- Los accesos deben ser solicitados y autorizados por el Gerente o Director de proceso al área de Tecnología la cual debe generar un ticket.

- El empleado es responsable de sus credenciales y debe asumir la responsabilidad del acceso otorgado asegurando el uso adecuado de este.

- Es responsabilidad de cada Gerencia o área dueña de proceso, el mantenimiento de los roles y privilegios configurados o asignados a los diferentes activos de información por medio de la SIGO-SI-13.2-IA-FR Matriz de Roles y Privilegios, esta revisión se recertificará semestralmente.

- El líder de proceso con la colaboración del proceso de Talento Humano, deberán gestionar la baja de los identificadores de los empleados propios que hayan terminado su relación laboral con la empresa.

- Utilizar contraseñas robustas seguras y cambiarlas frecuentemente o cuando se sospeche que han sido comprometidas.

Control de Accesos

- No se permite que varios usuarios compartan el mismo identificador (denominados usuarios genéricos) en la red o diferentes sistemas de información de Corredor Empresarial S.A.
- No compartir las credenciales de acceso asignadas a los diferentes sistemas o aplicaciones.
- No utilizar los usuarios o contraseñas que vienen por defecto en los sistemas de información.
- Las credenciales de acceso No deben ser escritas, copiadas o reproducidas en papel o en un documento electrónico sin protección.
- Se prohíbe la conexión de dispositivos de almacenamiento externos, tales como memorias USB, dispositivos de almacenamiento extraíbles y discos duros portátiles.

Seguridad en Redes y Comunicaciones

- Impedir la conexión directa de entrada o salida de tráfico entre Internet y las redes de la Compañía.
- Habilitar sólo servicios y protocolos seguros que sean necesarios según lo requiera la función del sistema.
- El acceso a la red por parte de Visitantes (Clientes, Proveedores y cualquier personal externo) en la compañía, sólo está autorizado por medio de la red inalámbrica creada para tal fin.
- La conexión remota a la red de área local de Corredor Empresarial S.A, debe realizarse a través de una conexión segura.
- Es responsabilidad del área o dueño del proceso informar al área de Tecnología e Infraestructura, para realizar la desactivación o renovación de los servicios de conexión de terceros.
- No está autorizado el uso o implementación de redes inalámbricas independientes (Router, Modems o de tipo AD HOC), entre dispositivos que puedan acceder a la información o a las redes internas de la compañía.

Escritorio y Pantalla Limpios

Para mantener la confidencialidad, integridad y disponibilidad de la información, los empleados deberán mantener buenas prácticas de seguridad en su puesto de trabajo:

- En el momento de la asignación de un activo, el empleado se convierte en su custodio y responsable.
- Guardar bajo llave la información sensible en papel o almacenada en soportes digitales.
- Bloquear la sesión de trabajo del equipo de cómputo al ausentarse del puesto de trabajo.
- No navegar por sitios no confiables o que puedan facilitar la propagación de virus y/o spam, descargar y/o instalar software o material protegido con las restricciones de propiedad intelectual sin la correspondiente licencia de uso, intercambiar información sensible sin una protección adecuada, etc.
- No publicar información de la empresa (documentos, videos, opiniones, etc.) sin autorización en servidores públicos de Internet.

Respaldo de Información

El área de Tecnología e Infraestructura definirá los programas de respaldo de información con tiempos de retención. Las retenciones adicionales a las definidas deberán ser confirmadas al área de Tecnología por los líderes de los procesos de la compañía.

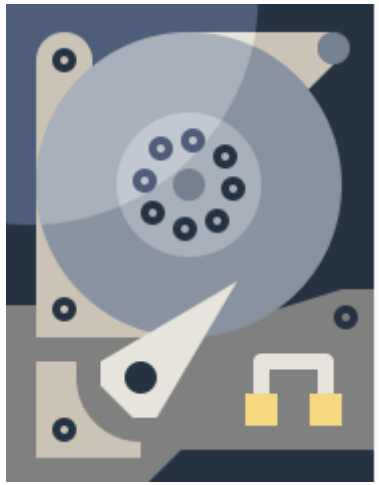
Todas las copias de seguridad de la información Reservada o Confidencial deben ser almacenadas en un área aprobada con acceso controlado y condiciones ambientales adecuadas que garanticen su preservación.

Las copias de respaldo deben ser custodiadas en una instalación diferente al sitio de procesamiento de la información, con el fin de garantizar la continuidad del negocio.

- Es necesario que los medios magnéticos y ópticos sean correctamente etiquetados y organizados para facilitar su identificación y ubicación en el momento en que se requiera recuperar información.
- El área de Tecnología e Infraestructura debe documentar los procesos de ejecución de restauraciones de copias de seguridad para cada tipo de información a respaldar.

Eliminación de Información

Las solicitudes de destrucción o eliminación de información pueden generarse desde las áreas internas o por parte de sus clientes.



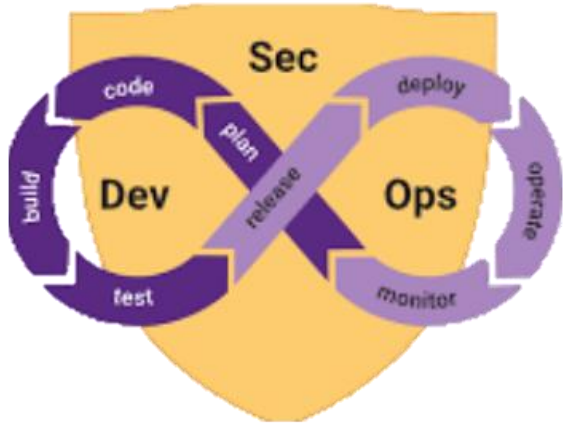
- La información propia de la compañía, sólo se podrá eliminar o destruir con autorización previa del comité de gestión documental, líder de área y la validación del dueño del proceso y que no vaya en contravía de la normatividad vigente o acuerdos contractuales con partes interesadas.

Desarrollo Seguro

El área de Tecnología y Desarrollo establecerá claramente los requerimientos funcionales, operacionales y especificaciones técnicas para la adquisición o desarrollo de sistemas de información y/o comunicaciones, contemplando requerimientos de seguridad de la información.

- Se debe contar con ambientes independientes de Desarrollo, Pruebas y Producción para el desarrollo de software, estos deben contemplar controles físicos y de acceso lógico para garantizar la separación de los mismos.
- Utilizar cuentas de usuario diferentes para los ambientes de desarrollo, pruebas, y producción (las mismas deben cumplir con los criterios del uso adecuado de contraseñas).
- Desarrollos inventariados, plenamente documentados y registrados legalmente.
- Se debe restringir y auditar el acceso a los repositorios del código fuente de los desarrollos.

DevSecOps



sonarqube

OWASP TOP 10

Como parte de las actividades del ciclo de vida del desarrollo se deben tomar como referencia, prácticas reconocidas de codificación segura (ejemplo: OWASP, NIST 800, SANS CWE Top 25, CERT Secure Coding, etc).

Incidentes de Seguridad de la Información

Todos los empleados de Corredor Empresarial S.A., son responsables de reportar debilidades, eventos e incidentes de Seguridad de Información de los cuales tengan conocimiento en las plataformas, activos de información digitales o los mismos activos de información físicos que estén bajo su cargo.

- Se establece un **Equipo de Gestión de Incidentes** de seguridad de la compañía, estará conformado como mínimo por:

  - ✓ El propietario y/o custodio del activo
  - ✓ El profesional o equipo de la gerencia de Tecnología que apoya la gestión de incidentes de seguridad
  - ✓ El Oficial de Seguridad de la Información
  - ✓ Demás profesionales de las áreas de la compañía que tengan a cargo activos o procesos que se vean afectados por el incidente
  - ✓ Además el profesional de la gerencia Oficial de Cumplimiento que participará si se ve afectada una base de datos con datos personales o información sensible.

- El Equipo de Gestión a incidentes podrá solicitar la participación de otros empleados, procesos, especialistas y/o terceros requeridos para la atención del incidente de seguridad.

Inspecciones de Seguridad de la Información

El objetivo de las inspecciones de Seguridad de la Información es el de validar con los diferentes procesos de Corredor Empresarial S.A., la aplicación de las políticas y normatividad interna; también identificar nuevos riesgos, vulnerabilidades o incidentes relacionados con la Seguridad de la Información.

Es responsabilidad de los dueños o líderes de procesos realizar seguimiento a las acciones correctivas, preventivas y planes de remediación que puedan ser generados como resultado de estas inspecciones y pruebas aplicadas.

Las áreas técnicas y de control de Corredor Empresarial S.A. podrán realizar las siguientes actividades para validar el estado del cumplimento de lo emanado por seguridad de la información:

- **Auditorias de cumplimiento o periódicas bajo el estándar ISO 27001:2022 que se debe realizar mínimo una vez al año para la verificación del estado del cumplimiento.** Las auditorias serán realizadas por auditores internos o externos según aplique.
- **Test de Penetración o pruebas de Ethical Hacking** como validación de las medidas de seguridad de la información en la infraestructura tecnológica de la compañía, los cuáles serán ejecutadas por un tercero, quien generará el informe correspondiente para que se establezca el plan de remediación.
- **El área de Tecnología debe realizar revisiones periódicas** para verificar que los sistemas de información cumplan con lo emanado por seguridad de la información.

Seguridad Física

La seguridad física protege a las personas, instalaciones y activos contra amenazas físicas, asegurando la integridad y continuidad operativa.

- Es obligatorio registrar el ingreso de los visitantes y segur el protocolo de seguridad para su acceso a las instalaciones.
- Es obligatorio registrar el ingreso y la salida mediante el sistema biométrico de acceso.
- Informar inmediatamente sobre cualquier actividad o persona sospechosa
- No divulgar información confidencial o sensible.
- Respetar las políticas de no acceso a áreas restringidas sin autorización.
- Respetar las políticas y normas de acceso de visitantes.
- No dejar dispositivos electrónicos desatendidos.
- Bloqueo de equipos de cómputo cuando no estén en uso.
- No conectar dispositivos USB desconocidos a las computadoras de la empresa.

Anonimización de datos

La anonimización es el proceso de eliminar o modificar información personal identificable de un conjunto de datos, de manera que las personas a las que se refiere no puedan ser identificadas directa o indirectamente.

Enmascarado de datos (blacklining)

First name	Last name	CC number
Denise	Smith	5248 6842 2178 3954
Monica	Hanraets	5830 8506 1640 3677
Youri	Soler	3226 4901 4892 9975
Stella	Montagna	9757 6035 3687 6841
Hamlet	Donnelly	6901 0354 6872 9865
Soraya	Lachance	1778 6983 2647 3205

First name	Last name	CC number
Denise	Smith	[redacted] 3954
Monica	Hanraets	[redacted] 3677
Youri	Soler	[redacted] 9975
Stella	Montagna	[redacted] 6841
Hamlet	Donnelly	[redacted] 9865
Soraya	Lachance	[redacted] 3205

Anulación (borrado)

First name	Last name	Middle name
Denise	Smith	Joanna
Monica	Hanraets	Elena
Youri	Soler	Michael
Stella	Montagna	Valerie
Hamlet	Donnelly	René
Soraya	Lachance	Violet

First name	Last name	Middle name
Denise	Smith	NULL
Monica	Hanraets	NULL
Youri	Soler	NULL
Stella	Montagna	NULL
Hamlet	Donnelly	NULL
Soraya	Lachance	NULL

Encriptación de datos

First name	Last name	CC number
Denise	Smith	5248 6842 2178 3954
Monica	Hanraets	5830 8506 1640 3677
Youri	Soler	3226 4901 4892 9975
Stella	Montagna	9757 6035 3687 6841
Hamlet	Donnelly	6901 0354 6872 9865
Soraya	Lachance	1778 6983 2647 3205

First name	Last name	CC number
Denise	Smith	Ð?Ω𝑟ą𝑍&-ü02#a$/®¶𝑛́
Monica	Hanraets	ßg6]»¥Ɇę̈Q)å⁰<⅞¢¤Ũə
Youri	Soler	ĵ¦+Ƙ4Ł̃Ěá$ffThO0;þiɲ!
Stella	Montagna	áJř6*`C≠√uẄĜ@0ẽ¿2
Hamlet	Donnelly	h=⅔Ďg̈t\~RijÅß{“™Ũè-
Soraya	Lachance	3Ÿ®>¤µbG̃ák^,ƒĩŤÖc4}

Estas fotos son del Autor: www.klippa.com