CORREDOR EMPRESARIAL S.A.

Políticas de la Seguridad de la Información

Por qué de la Seguridad de la Información?

La información es el activo más importante después de los empleados con el cual la compañía soporta sus procesos para alcanzar sus objetivos críticos; la **Seguridad de la Información** busca protegerla de:

- 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

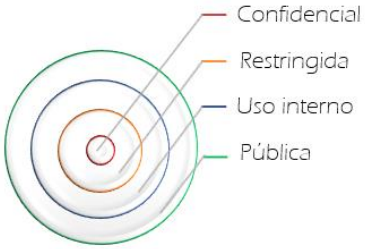
- Contar con usuario y contraseña y velar por que la información almacenada en el equipo se encuentre debidamente cifrada o protegida.
- Los dispositivos móviles no corporativos se considerarán como inseguros por defecto y no podrán conectarse a ninguna red corporativa, ya sea esta cableada o inalámbrica, 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, impresa, 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.



- Los activos de información de Corredor Empresarial S.A. deben ser preservados y únicamente deben ser utilizados para propósitos relacionados con el negocio de la empresa.

Control de Accesos

- Tener procedimientos para acceso físico 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.

- Todo identificador debe estar relacionado con un usuario físico con el propósito de reconocer y comprobar la identidad del usuario que accede, de forma inequívoca y personalizada para que sea responsable de su uso.

- 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.

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).

Las páginas web publicadas en Internet deben contar con certificado digital emitido por una entidad certificadora externa, avalada internacionalmente.

Las páginas web publicadas internamente deben contar con un certificado digital, emitido por una entidad certificadora interna.

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.

Bogotá | 20 Feb 2012 - 7:46 am

Inseguridad en Bogotá

Computadores robados a directora del IDU tienen información de carrusel de contratos

La Policía investiga el caso.

Por: Elespectador.com

96
Compartido

María Fernanda Rojas, directora del Instituto de Desarrollo Urbano

Seguridad en Redes y Comunicaciones

- La red de Corredor Empresarial S.A. deberá estar debidamente documentada con diagramas y topologías, mostrando los nodos y sus conexiones, al momento de ingresar o configurar un nuevo dispositivo de red se debe actualizar la documentación mencionada.
- Se establece una base para la segmentación de las subredes corporativas en:
  - **Red de Usuarios**
  - **Red de Administración y Monitoreo**
  - **Zona Desmilitarizada (DMZ)**
  - **Red inalámbrica Interna**
  - **Red inalámbrica Visitantes**
  - **Red de Impresión**
  - **Red de Seguridad física y CCTV**
- Configurar los equipos de cómputo, infraestructura y telecomunicaciones de la compañía con base en las guías de hardening o configuración segura publicadas por los fabricantes o la industria.

- Para establecer una conexión a la red de Corredor Empresarial S.A. por parte de proveedores, clientes o partes interesadas; deben establecerse canales dedicados o enlaces tipo VPN (Site to Site).
- Las solicitudes de conexiones externas que presenten algún tipo de riesgo o incumplan las reglas establecidas en este documento deben ser aprobadas por el Comité de Riesgos y Seguridad de la información.
- Validar que toda regla en el Firewall y uso de todos los protocolos no seguros (HTTP, FTP, Telnet, IMAP, POP3, SNMP, entre otros) se encuentren documentados y justificados.
- Mantener actualizado todos los equipos de cómputo de la compañía actualizados y con los últimos parches de seguridad.
- Tener en cuenta las directrices indicadas en las políticas de “Control de Acceso” y “Dispositivos Móviles, Teletrabajo y Trabajo en Casa” con sus estándares derivados.

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 (AD HOC), entre dispositivos que puedan acceder a la información o a las redes internas de la compañía.

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.

El líder de proceso propietario de la información debe informar al área de Tecnología sobre la necesidad de respaldo y tiempo de retención de su información

Eliminación de Información

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

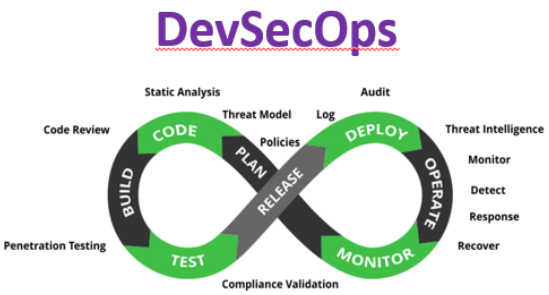
- La información propia de la compañía, sólo se podrá eliminar o destruir con autorización previa del Gerente o director de área y la validación del dueño del proceso y que no vaya en contravía de la normatividad vigente o acuerdos contractuales con partes interesadas.
- Cuando exista la necesidad de dar de baja medios de almacenamiento tales como: CDs, DVDs, discos duros, discos extraíbles, discos USB u otros, que hayan contenido información confidencial de la compañía deberá realizarse un proceso de eliminación segura de información anterior a su destrucción física.
- Posterior al borrado seguro de la información, se puede proceder a reutilizar el elemento.

Cuando la eliminación o destrucción de Información sea realizada por un tercero contratado para tal fin, se solicitará al tercero una certificación formal de la destrucción como evidencia de la misma.

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.
- No deben utilizarse datos reales de producción en ambientes de pruebas. En caso de ser requerido se debe realizar un procedimiento de ofuscamiento de datos para garantizar la seguridad de los datos en producción o contar con los mismos controles que se tienen en producción para los otros ambientes.
- Para todos los sistemas desarrollados, se debe implementar un proceso de verificación automático de código durante el desarrollo y una análisis de vulnerabilidades de seguridad antes de su salida a producción. Toda vulnerabilidad crítica, alta o media en la infraestructura debe ser solucionada antes de su paso a producción.
- En caso que el desarrollo sea realizado por un tercero, este debe presentar certificación de la revisión de código y análisis de vulnerabilidades de seguridad donde se certifique que la aplicación no cuenta con vulnerabilidades



OWASP
Open Web Application Security Project

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.


22 Nov 2021

elCOLOMBIANO

ANTIOQUIA COLOMBIA MUNDO ECONOMÍA DEPORTES OPINIÓN CULTURA TENDENCIAS TECNOLO

Ataque cibernético al Dane causó pérdida de información "sensible"

- 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.

- Mensaje a los correos electrónicos Soporte@cemcolombia.co, Noc@cemcolombia.co y Oficialseguridaddeinformacion@cempresarial.co
- A través del módulo de la herramienta de helpdesk Osticket
- Mensaje a la línea de atención por WhatsApp **3175031234**.

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.

- 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.
- Estas inspecciones serán periódicas, no programadas y de manera aleatoria a los diferentes procesos de la compañía. Se debe generar un informe con las principales recomendaciones u oportunidades de mejora identificadas y con base en este informe se deben realizar los ajustes correspondientes por parte de los líderes o dueños de los procesos objeto de la inspección.

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 27001:2013 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.

GRACIAS