



Information Security

Código de Práctica

Global Template
< version 1.0 >



Contenido

1. Introducción
2. Seguridad de la Información en General
3. Reporte de Incidentes de Seguridad
4. Clasificación de Activos
5. Seguridad Física y Ambiental
6. Hardware y Software
7. Control de Acceso al Sistema
8. Uso del Correo Electrónico y Acceso a la Web
9. Computadoras Móviles / Teletrabajo
10. Incumplimiento
11. Declaración
12. Términos, Definiciones y Referencias
 - 12.1 Términos y Definiciones
 - 12.2 Documentos Referidos

Introducción

Los empleados de DHL tienen acceso a sistemas de computación y de comunicación críticos así como también a datos potencialmente sensibles y valiosos. Este Código de Práctica en materia de Seguridad de la Información (COP) es obligatorio para todos los empleados, consultores y contratistas que trabajan para DHL. Debe entenderse que los términos "persona" y "usuario" incluyen a los empleados, consultores y contratistas.

Estas disposiciones, en los casos en que corresponda, continuarán siendo obligatorias con posterioridad a la finalización de la relación laboral de la persona con DHL. Ninguna persona empleada por DHL podrá divulgar la información que no sea de carácter público acerca de DHL, sus clientes o proveedores.

Este Código de Práctica abarca toda responsabilidad del usuario tal como se la define en el Estándar de Seguridad de Información de Línea de Base (BISS) de DHL y debe ser firmado por toda persona antes de tener acceso a la infraestructura informática de DHL. Los números entre corchetes [números] hacen referencia al BISS.

Es importante que toda persona adhiera a los estándares de ética y siga las normas que contribuyen al éxito y a la imagen de la marca de DHL. La falta de cumplimiento del COP podría traer aparejadas serias consecuencias para DHL así como para las personas que trabajan en ella. Se requiere la colaboración de todos los empleados para lograr un ambiente de trabajo seguro.

Si tiene alguna duda con respecto a este Código de Práctica, sírvase dirigirse a su Gerente de Seguridad de Información Local.





Seguridad de la Información en General

■ Con el fin de proteger la información confidencial de DHL, todas las personas deben firmar un acuerdo de confidencialidad por el cual:

■ Toda persona acuerde cumplir con las obligaciones y responsabilidades de seguridad que se describen en la correspondiente descripción de su puesto de trabajo (job description).

■ Toda persona acuerde ser responsable del uso razonable y adecuado de los sistemas de servicios de información (IS) de DHL, de los activos de información y de los servicios de información de sistemas en general.

Los sistemas y servicios de información (IS) incluyen, sin limitación, computadoras, correo electrónico, teléfonos, casillas de mensajes, teléfonos celulares, organizadores personales, máquinas de fax, boletines electrónicos externos, servicios de comunicación por cable, servicios on-line, Intranet e Internet (World Wide Web).

■ Toda persona se responsabilice por el cumplimiento de las disposiciones aplicables en materia de seguridad con respecto a la información corporativa y acuerde cumplir con los estándares específicos de DHL así como con las instrucciones impartidas por los titulares o dueños de la Información.

■ Toda persona acuerde asistir a los cursos de capacitación en materia de seguridad que generalmente se llevan a cabo durante el periodo de inducción con el fin de la persona entienda las políticas de DHL.

■ Toda persona tenga acceso solamente a la información que resulte necesaria para su trabajo. Todo aquel que tuviera acceso a información que debiera ser protegida y que no fuera necesaria para el trabajo por el desarrollado en ese momento, deberá informar esta situación a la Mesa de Ayudas (Helpdesk) de inmediato.

■ Cuando una persona deje la organización, se comprometa a devolver todo el software, hardware, documentos y medios que se pudieran encontrar en su poder debido a su relación laboral o comercial con DHL. La persona que abandone la empresa no podrá retener copias de la información de propiedad de DHL. Todos los permisos de acceso a los recursos de servicios de información (IS) que fueran otorgados a un empleado de DHL durante su relación laboral serán revocados de inmediato al concluir dicha relación laboral.



UTILICE LOS SISTEMAS DE DHL DE MANERA RAZONABLE



Reporte de Incidentes de Seguridad

- [6.4.3] **■** Toda persona debe estar familiarizada con el procedimiento local para el reporte de incidentes de seguridad. Los incidentes técnicos de seguridad deben ser informados a la Mesa de Ayudas (Helpdesk). Todos los demás tipos de incidentes de seguridad deben ser informados al LISM, de ser apropiado

Ejemplos de incidentes técnicos de seguridad:

- Pérdida o robo de equipos de sistemas
- Virus de computadora
- Software y sistemas que no operan en la forma esperada

Ejemplos de otros tipos de incidentes de seguridad:

- Incumplimiento de las políticas y estándares de DHL
- Comportamiento inusual de personas

- [6.4.4] **■** Ninguna persona podrá tratar de explorar ni demostrar una debilidad sospechada sin la autorización apropiada. La verificación de debilidades es interpretada como un uso inadecuado del sistema.
- Toda persona que reciba una advertencia informal acerca de una potencial amenaza a la seguridad, como por ejemplo, un virus peligroso proveniente de los medios, familiares o amigos o contactos comerciales fuera de DHL, deberá informarlo de inmediato a la Mesa de Ayudas (Helpdesk). Ninguna persona que no pertenezca a la Mesa de Ayudas podrá notificar directamente a los asociados de DHL ni a ningún otro contacto interno acerca de una posible amenaza.



- ✓ **INFORME TODO COMPORTAMIENTO SOSPECHOSO O INUSUAL DE UN SISTEMA A LA MESA DE AYUDAS (HELPEDESK)**
- ✗ **NO EXPLORÉ DEBILIDADES EN LOS SISTEMAS DE DHL - TAL ACCIONAR SERA INTERPRETADO COMO UN USO INDEBIDO O INAPROPIADO DE LOS SISTEMAS**



Clasificación de Confidencialidad de los Activos

- Para poder asegurar el uso responsable de los principales activos de información, el propietario de la información debe clasificar los activos de acuerdo con los niveles de confidencialidad de DHL [5.1]
- Niveles de Confidencialidad:
 - **Información Pública** [5.2.3.1]

Definición: Información que no se encuentra comprendida dentro de los restantes niveles. Esta información es pública o su divulgación no dañaría a la compañía ni a ningún otro individuo. Información, cuya divulgación pública se encuentra específicamente autorizada.

Ejemplos: Información sobre relaciones públicas, folletos, informes de la compañía, materiales de cursos y seminarios, materiales de exhibición.
 - **Información para Uso Interno de DHL:** [5.2.3.2]

Definición: Información de propiedad de la compañía, cuya divulgación a otra compañía o persona diferentes de aquellas personas que necesitan tener acceso a la misma para su trabajo, podría resultar en un daño menor para la compañía. Este es un nivel de confidencialidad mínimo, por default, para la totalidad de la información de DHL.

Ejemplos: programas de vuelos, bases de carga, números de teléfonos internos, informes, circulares, material de capacitación interna, manuales de DHL, programas de marketing de DHL, documentación preliminar, información de proyectos, informes de progresos o avances, informes de calidad.
 - **Información Confidencial de DHL:** [5.2.3.3]

Definición: Información de propiedad exclusiva que si fuera divulgada fuera del grupo funcional o de la comunidad de DHL, podría resultar en un daño serio para la información de DHL, que se encuentra sujeta a obligaciones de privacidad contractuales o requerimientos de privacidad establecidos por las leyes o las reglamentaciones vigentes.

Ejemplos: Información acerca de los sueldos, salarios y beneficios de los empleados, códigos fuente de software, planes tácticos, programas de marketing, documentación preliminar, información de proyectos, informes de progreso, informes de calidad, cronogramas de descuentos o precios especiales, información acerca de inteligencia de mercado en general, informes sobre rutinas de seguridad, detalles de implementación y diseño de sistemas de seguridad, (firewalls, control de acceso, diagramas de red, etc.), y toda otra información que sea clasificada como "para uso interno de DHL exclusivamente".
 - **Información Secreta de DHL:** [5.2.3.4]

Definición: Información de propiedad exclusiva de DHL que, si fuera divulgada a una empresa o persona diferentes de aquellos empleados que deban tener acceso

a la información para el desarrollo de sus actividades y quienes han sido autorizados expresamente a recibirla por su propietario, resultaría en un daño sustancial a DHL, Deutsche Post World Net, sus clientes, personal o socios. Información que debería ofrecer una ventaja comercial significativa a un competidor, y toda información que, si fuera divulgada, causaría daños significativos.

Ejemplos: estrategias de marketing, datos de investigación, planes de estrategias comerciales, proyecciones, tarifas especiales, factores de conversión de carga, secretos comerciales, resultados financieros, especificaciones de productos, inteligencia específica de mercado y de la competencia, informes de incidentes serios de seguridad, clasificaciones de crédito de clientes transnacionales, información impositiva del país, documentación legal, futuras protecciones de marcas, y estrategias de productos, planes de compra o venta de compañías o subsidiarias.

[5.2.6] ■ Toda persona deberá tratar la información de acuerdo con su clasificación. En caso de no estar seguro acerca del tratamiento de la información, será necesario contactar a su propietario.

■ Definiciones

- Daño Menor - daño comercial no específico, directo y mensurable. Un incumplimiento de la obligación de seguridad a este nivel podría crear sospechas acerca de una pobre administración de la compañía. Una sucesión de incidentes que causen daños menores podrían causar un daño mayor a largo plazo. Podría afectar la moral de los empleados más que la rentabilidad de la empresa.
- Daño Serio - pérdida notable de negocios o recursos que pueden ser reparados/recuperados, demoras en los proyectos o desarrollos clave, relación con algunos clientes afectados, violación menor a una obligación contractual o a un requerimiento establecido por ley o reglamentación, daño no significativo a la reputación.
- Daño Sustancial - implica un efecto sustancial sobre las ganancias de la compañía y trae aparejado la reparación de la imagen pública y comercial. Podría implicar la pérdida de una posición en el Mercado, la pérdida de personal clave, la suspensión de los proyectos o desarrollos clave, acciones legales dadas a conocer al público, impacto significativo sobre la reputación para la integridad comercial y atención al cliente.

Procedimiento de Administración de Información Clasificada	Pública	Para uso interno de DHL únicamente	Confidencial de DHL	Secreta de DHL
Circulación				
Sólo a criterio del autor - sin copias			✓	✓
A criterio de la lista de distribución - Nombres			✓	✓
Uso interno - personal que necesita estar informado		✓		
Disponibilidad para el público en general	✓			
Método de circulación				
Copia impresa	✓	✓	✓	✓
Medios electrónicos removibles como por ejemplo, aunque sin limitarse a: disquete, CD, DVD, USB Stick, cintas y discos duros externos	✓	✓ ***	✓ ***	✗
Por correo electrónico	✓	✓	✗	✗
Por correo electrónico encriptado	✓	✓	✓	✗
Por Intranet con control/ autenticación de acceso	✓	✓	✓	✗
Servidor aprobado para guardar información Confidencial*	✓	✓	✓	✗
Servidor aprobado para guardar datos secretos*	✓	✓	✓	✓
Herramientas de colaboración	✓	✓	✗	✗
Por Intranet sin control / autenticación de acceso	✓	✗	✗	✗
Disponible en el sitio de Internet de la compañía	✓	✗	✗	✗
Almacenamiento en la PC de la empresa	✓	✓	✓ **	✗
Almacenamiento en PDA o teléfono celular de la empresa	✓	✓	✓ **	✗

* Consulte a la Mesa de Ayudas (Helpdesk) qué servidores son seguros y se encuentran aprobados para procesar la información confidencial o secreta.

** Sólo si la PC se encuentra aprobada para procesar y almacenar datos confidenciales. Pregunte a su Mesa de Ayudas (Helpdesk)

*** Sólo si el medio es controlado por DHL y el método de almacenamiento es aprobado. Consulte a su Mesa de Ayudas (Helpdesk)

✗ No permitida



- ✗ NO ENVIE INFORMACION CONFIDENCIAL FUERA DE DHL
 - ✗ NO HAGA COPIAS DE LOS DATOS A MEDIOS REMOVIBLES NO AUTORIZADOS, COMO POR EJEMPLO, CD, DVD, USB-STICK
 - ✓ DISPONGA DE LA INFORMACION A TRAVÉS DE LOS MEDIOS ADECUADOS
- CONSULTE A LA MESA DE AYUDAS (HELPPDESK)



Seguridad Física y Ambiental

- [7.1.2] ■ Toda persona debe usar en forma visible la identificación mientras se encuentre en las instalaciones de DHL.
- No se deben compartir con otras personas los números PIN ni las tarjetas de acceso. Por razones de seguridad, se encuentra estrictamente prohibido el ingreso a las instalaciones junto a otra persona sin utilizar la tarjeta propia cuando ésta ingresa su contraseña personal de acceso.
- [7.1.4] ■ Se deben registrar a todas las visitas. Además, deben estar siempre acompañadas cuando se encuentran en áreas sensibles. Entre las áreas sensibles se incluyen el centro de datos, NOC, y las salas técnicas. No se aconsejan las visitas guiadas por las áreas sensibles y cuando se lleven a cabo, deberán contar con la autorización de los directivos.
- [6.4.2] ■ Dentro de las instalaciones de DHL, es aconsejable no dejar pasar a aquellas personas que no cuenten con una identificación en un lugar visible.
- Toda persona debe asegurarse de que su equipo controlado por DHL se encuentre protegido mientras no esté en uso.
- [7.3.1] ■ Toda persona debe cumplir con la "política de escritorios y pantallas limpias":
 - La información comercial sensible o crítica y los medios de computación deben ser almacenados en forma segura mientras no sean utilizados.
 - Cuando se encuentre en la oficina, las computadoras portátiles que sean utilizadas deben ser aseguradas con un cable de bloqueo (cable lock). Las computadoras portátiles que permanezcan en las instalaciones deben estar en todo momento protegidas bajo llave.
 - Las impresiones deben ser removidas de las impresoras de inmediato.
 - Los usuarios deben activar los protectores de pantalla automáticos y bloquear o desconectar sus estaciones de trabajo toda vez que dejen sus escritorios temporalmente. La activación automática de los protectores de pantalla no es suficiente ya que deja a los sistemas desprotegidos durante varios minutos.
 - Los usuarios deben asegurarse de haber desconectado todos los sistemas antes de retirarse de las instalaciones.
- [7.3.2] ■ Sin la autorización de los directivos, los empleados no podrán retirar fuera de las instalaciones los equipos, datos ni el software de la compañía.
- [7.2.5] ■ Las computadoras portátiles (por ejemplo las notebooks, Asistentes Personales/PDA, etc.) así como los medios de computación que sean utilizados fuera de las instalaciones, deben estar protegidos en todo momento. (cf. 9. Computadoras portátiles / Teletrabajo.
- [7.2.6] ■ Para asegurarse la disposición o reutilización segura de los equipos que contengan información sensible, confidencial o datos clasificados o secretos, el usuario deberá contactarse con la Mesa de Ayuda (Helpdesk) y solicitar las instrucciones necesarias.
- [8.5.1] ■ Los equipos conectados a la red DHLNet no deben tener acceso simultáneo a otras redes.
- [9.3.1] ■ Toda persona deberá asegurarse de que solo se conecte el equipo de propiedad de DHL a la red DHLNet, de acuerdo con los estándares de DHL. Toda excepción requerirá la previa aprobación de la Gerencia de Seguridad Informática Local. (LISM).



- ✓ DESCONECTE SU COMPUTADORA O UTILICE UN PROTECTOR DE PANTALLA CON PASSWORD MIENTRAS NO LA ESTE UTILIZANDO.
- ✓ ORDENE SU ESCRITORIO AL FINAL DEL DIA Y CIERRE CON LLAVE TODOS LOS CAJONES Y GABINETES.
- ✓ PROTEJA SU COMPUTADORA Y LA INFORMACION EN ELLA CONTENIDA DE TODA CLASE DE HURTO, DAÑO Y USO INDEBIDO.
- ✗ NO DEJE DISQUETTES NI OTRO TIPO DE INFORMACION POR LOS ALREDEDORES - RECOJA TODAS LAS IMPRESIONES DE LA IMPRESORA DE INMEDIATO.
- ✗ NO CONECTE A LA RED EQUIPOS QUE NO SEAN CONTROLADOS POR DHL.
- ✓ FAMILIARÍCESE CON LOS PROCEDIMIENTOS DE EMERGENCIA.



Hardware y Software

- [12.1.5] ■ DHL lleva un inventario de los equipos entregados a cada uno de los usuarios. Toda persona tiene el derecho a examinar y corregir la información contenida en su inventario personal.
- Se desalienta el uso de los sistemas DHL IS (incluyendo el hardware y software) para fines diferentes de los de DHL (por ejemplo para uso privado) y el uso de tales equipos se permitirá en forma restringida. En todos los casos se requerirá la aprobación escrita de los directivos.
 - Los empleados de DHL solo podrán utilizar computadoras personales, PDA's etc. que se encuentren bajo el control de DHL tanto para el almacenamiento como para el procesamiento de información de propiedad exclusiva de DHL.
 - Los equipos que no sean administrados por DHL (o por un tercero contratado para tal fin) no deberán conectarse a las redes de DHL. Esto incluye la conexión vía acceso remoto, por ejemplo de una computadora de uso privado en el hogar. Usted podrá contactar a la Mesa de Ayudas (Helpdesk) para solicitar excepciones temporarias en el caso de visitas y contratistas.
 - No se permite a los usuarios instalar ninguna especie de software en los equipos de DHL. Para instalar un software, siga el procedimiento apropiado o las instrucciones de la Mesa de Ayudas (Helpdesk) para mayor información.
 - El Software debe ser utilizado solamente para los fines para los que haya sido creado. No se pueden violar los derechos de autor ni los derechos de propiedad intelectual de DHL ni de terceros.
 - Para el uso del mecanismo de criptografía en los sistemas o software de DHL, el usuario debe contactar a la Mesa de Ayudas (Helpdesk) para mayor información.
 - Sólo se podrá utilizar software aprobado y bajo licencia.



- ✗ NO UTILICE COPIAS DE SOFTWARE PRIVADAS O NO AUTORIZADAS
- ✗ NO UTILICE COMPUTADORAS NI INFORMACION DE DHL PARA FINES PERSONALES - LAS COMPUTADORAS Y LA INFORMACION DE DHL SON PARA USO EXCLUSIVO DE LA EMPRESA
- ✗ NO HAGA COPIAS DE SOFTWARE NI DE LA INFORMACION PARA FINES PERSONALES



Control de Acceso al Sistema

- Toda persona es responsable de las actividades que se realicen con su clave personal (ID). No se debe compartir la clave personal (ID). No se permite a los usuarios utilizar la clave personal (ID) de otro usuario.
- Las credenciales utilizadas por los usuarios como, por ejemplo, las passwords o códigos (PIN) deben ser cambiadas periódicamente aún cuando el sistema no esté configurado de esta manera. La frecuencia por default es de cada 60 días. Se considera una frecuencia más alta en el caso de cuentas de usuarios con mayores privilegios y la clave se le comunica al usuario al momento de la distribución de las claves personales iniciales.
- Al confeccionar una contraseña personal (password) fuerte se deben aplicar las siguientes normas:
 - El largo mínimo de la clave es de 8 caracteres
 - La contraseña personal debe consistir de por lo menos:
 - Una mayúscula
 - Una minúscula y
 - Un número
 - Las claves personales no deben ser re-utilizadas. Es probable que el sistema aliente esta práctica.
 - Las claves personales no deben estar basadas en datos personales. Otras personas podrían adivinar fácilmente su clave o contraseña al obtener información relacionada con su familia, por ejemplo, nombres de la esposa o esposo, hijos, números de teléfonos, domicilios, fechas de cumpleaños, etc.
- Para una autenticación basada en la contraseña personal, los usuarios reciben una contraseña temporaria segura que debe ser cambiada por el usuario inmediatamente después de conectarse con su propia clave.
- Los usuarios deben cumplir con las siguientes normas con respecto al uso de las credenciales:
 - Las credenciales se clasifican como "Información Confidencial de DHL"; las credenciales son personales y nunca deben ser divulgadas; los usuarios son responsables de toda acción que se lleve a cabo con cualquiera de sus cuentas de usuario.
 - Las credenciales no deben conservarse en papel o en medios de computación, a menos que puedan ser almacenadas en forma segura. Las claves personales (passwords) no deben ser distribuidas a través de correos electrónicos encriptados.
 - Las credenciales deben ser cambiadas toda vez que sean reveladas o cuando el sistema o la credencial se vieran comprometidos.
 - Las credenciales no deben incluirse en un proceso de conexión automática, por ejemplo, almacenadas en un macro o en una tecla de función. Toda vez que la computadora le pregunte si desea recordar la contraseña para un uso posterior, deberá contestar que no.
 - Las credenciales (passwords) utilizadas para tener acceso a los activos de DHL no deben ser re-utilizadas para un uso diferente del uso de DHL (por ejemplo, para acceder a su casilla de correo personal, a una computadora de uso privado o para tener acceso a un sitio web en la Internet).



- ✓ **MANTENGA SU CONTRASEÑA PERSONAL (PASSWORD) BAJO ESTRUCTAS CONDICIONES DE CONFIDENCIALIDAD Y CAMBIELA PERIODICAMENTE.**
- ✓ **CREE Y UTILICE CLAVES (PASSWORDS) FUERTES.**



Uso del Correo Electrónico y Acceso a Internet

- [9.7.1] ■ El acceso a Internet y a los sistemas de correos electrónicos proporcionados por la compañía debe ser utilizado como una herramienta que permita mejorar la ventaja comercial de DHL y a los usuarios llevar a cabo y cumplir con sus respectivas tareas. DHL controlará, de acuerdo con las leyes y reglamentaciones aplicables todas las operaciones relacionadas con el correo electrónico e Internet llevadas a cabo por los usuarios con el fin de planear la red, administrar el tráfico y la seguridad de estos sistemas. Los Usuarios no deben tener expectativas de privacidad con respecto a la información transmitida o recibida a través de las facilidades de Internet/Intranet y correo electrónico suministradas por DHL.
- El correo electrónico de DHL se debe utilizar en cumplimiento de las normas y reglamentaciones locales vigentes así como de las políticas y procedimientos de DHL. Se prohíbe el uso del correo electrónico para el envío o almacenamiento de mensajes irrespetuosos, obscenos, ofensivos, intimidatorios, amenazantes o para fines fraudulentos. DHL se reserva el derecho a bloquear todo correo electrónico que considere ofensivo o no relacionado con las operaciones comerciales de la empresa. Entre las comunicaciones electrónicas prohibidas se encuentran, sin limitación:
- El envío de documentos que violen leyes de propiedad intelectual;
 - El envío de material difamatorio acerca de la compañía o personas
 - El envío de material discriminatorio, racial, religioso o sexualmente ofensivo, amenazante o abusivo.
 - El envío intencional de un virus o bomba lógica.
 - El envío de "cadenas" de cartas.
 - El envío de información ilegal o contraria a los intereses de DHL.
- Todas las comunicaciones electrónicas transmitidas y almacenadas por medio de correos electrónicos son registros de propiedad de la compañía. DHL se reserva el derecho a acceder, utilizar, copiar y divulgar todos los mensajes enviados a través de sus sistemas de correo electrónico, independientemente de la finalidad de los mismos.
- El correo electrónico es como una tarjeta postal durante su transmisión, su contenido puede ser divulgado dentro de la red de propiedad de DHL o cuando sea transferido a través de Internet. La información confidencial o secreta de DHL no podrá ser enviada por correo electrónico.
- Los usuarios que se encuentren fuera de la oficina podrán hacer uso de los sistemas de correo electrónico denominados "Fuera de Oficina". Se prohíbe estrictamente el reenvío de correos electrónicos a direcciones de correo electrónico diferentes de las de DHL, a menos que se cuente con la aprobación del LISM.
- Los usuarios no deben enviar correos electrónicos en los que se presenten con otro nombre o identidad.
- Toda vez que un usuario reciba un correo electrónico basura, comúnmente denominados Spam, Scam o cadenas de cartas, deberá eliminarlo de inmediato y no podrá reenviarlo bajo ninguna circunstancia.
- Un usuario que reciba un correo electrónico con contenido ilegal o inadecuado, o un correo electrónico que contenga software malicioso, deberá informar de inmediato a

la Mesa de Ayudas (Helpdesk), esperar las instrucciones y no reenviarlo.

- El usuario no deberá verse tentado con la opción de responder un correo electrónico con la palabra "remove" cuando esta opción sea ofrecida, ya que de esta manera confirma que la dirección está activa y la hace más valiosa.
- Los usuarios deben retener los correos electrónicos que contengan datos comerciales relevantes por el tiempo requerido por las reglamentaciones vigentes.
- Los usuarios no deben utilizar su acceso a la Web para:
 - Ver o comunicar material de naturaleza obscena, discriminatoria o intimidatoria.
 - Llevar a cabo o incentivar una actividad comercial en beneficio personal.
 - Llevar a cabo actividades ilegales, incluyendo, los juegos de azar, la carga o descarga de software que viole los derechos de autor y/o software que estuviera sujeto a controles de exportación. Esto incluye la descarga de música, películas u otras clases de medios electrónicos.
 - Bajar e instalar software de Internet, incluso cuando esta actividad no viole los derechos de propiedad intelectual de terceros. Los usuarios que deban bajar o descargar software durante el curso de sus actividades comerciales deberán obtener las instrucciones adecuadas de la Mesa de Ayudas. (Helpdesk)
 - Intentar obtener el acceso no autorizado a otro sitio.
 - Verse involucrado en alguna actividad que viole las políticas de otra compañía o que estuviera en conflicto con los intereses de DHL.
 - Utilizar los denominados "tickers" u otros sitios activos (para obtener información, novedades de acciones, etc.), medios interactivos (por ejemplo, foros de discusión) y equipos de audio y video.
 - No contestar encuestas basadas en la web en representación de DHL, a menos que dichas encuestas hayan sido expresamente autorizadas por los directivos de la empresa.



- ✗ NO BAJE NI ALMACENE MEDIOS NO AUTORIZADOS COMO POR EJEMPLO, ARCHIVOS DE MUSICA Y VIDEOS EN SU EQUIPO CONTROLADO POR DHL.
- ✗ NO SE REENVIE DOCUMENTOS A UNA CUENTA DE CORREO ELECTRONICO FUERA DE DHL.
- ✗ NO ENVIE CORREOS ELECTRONICOS CON CONTENIDO ADVERSO A LOS INTERESES COMERCIALES DE DHL.
- ✗ NO ENVIE INFORMACION CONFIDENCIAL O SECRETA POR CORREO ELECTRONICO.
- ✗ NO RESPONDA A LOS CORREOS ELECTRONICOS BASURA O DENOMINADOS SPAM - LA CONTESTACION CONFIRMA LA RECEPCION VALIDA.
- ✗ NO DESCARGUE SOFTWARE POR SU CUENTA DE INTERNET - CONTACTE A LA MESA DE AYUDAS (HELPDESK)



Computadoras Móviles/ Teletrabajo

- [6.4.3] ■ Los usuarios son responsables de realizar una copia de seguridad (backup) de sus datos en forma regular, al menos una vez por semana. Las copias de seguridad deben estar adecuadamente protegidas contra hurto o pérdida de la información.
- Los usuarios no deben debilitar ni desactivar los sistemas de seguridad tales como el Antivirus o Firewalls.
- Los usuarios son responsables de asegurarse de que el Antivirus se encuentre actualizado con las nuevas firmas por lo menos una vez por semana. Los usuarios deben contactar de inmediato a la Mesa de Ayudas si sus firmas parecen tener más de una semana.
- No se deben utilizar equipos inalámbricos, tales como teléfonos celulares, PDA's y componentes de Red LAN inalámbrica o Bluetooth para conectarse a la Red DHLNet ni a ningún otro sistema de DHL sin la aprobación ni el software de conexión adecuado, como por ejemplo una red privada virtual (VPN).
- [6.4.4] ■ Nunca active la función compartir documentos en una PC. Esta función facilita el ingreso de un tercero a los datos compartidos o la instalación de software de naturaleza maliciosa en su sistema. La protección de los datos compartidos mediante una contraseña (password) no es de utilidad debido a algunas fallas que han sido detectadas en los sistemas de Microsoft, que permiten que las contraseñas puedan ser evitadas
- Las computadoras portátiles deben ser observadas en todo momento, a menos que se encuentren almacenadas o aseguradas con el cable de bloqueo (cable lock) recomendado. Esta norma se aplica a todas las situaciones estacionarias, incluidas, oficinas, habitaciones de hotel, escritorios en hogares, etc.
- Los usuarios deben asegurarse de practicar un estricto control de seguridad cuando se encuentren viajando con computadoras. Las computadoras deben ser observadas en todo momento y no deben exponerse a situaciones que pudieran generar un mayor riesgo de hurto, como por ejemplo, dejarlas en un auto estacionado. Cuando aborde un avión, las computadoras portátiles deben ser transportadas en la cabina en un lugar en el que puedan ser controladas por el usuario.
- Las computadoras portátiles pueden ser utilizadas para comunicarse por medio de un módem o de un adaptador de LAN. Todas las conexiones deben estar restringidas a los asuntos comerciales y a los servicios prestados por DHL. Estos incluyen los servicios de acceso remoto seguro de DHL.
- Cuando se encuentran conectados a DHL a través de VPN, los usuarios tienen acceso a los mismos recursos de Internet e Intranet que cuentan cuando se encuentran trabajando en sus oficinas. Se encuentran protegidos de acuerdo con los estándares de seguridad que cuentan las conexiones de la oficina.
- Cuando los usuarios se encuentren conectados a través de una conexión de discado o de banda ancha, la conexión debe establecerse a través del software de acceso DHL VPN. Este software DHL VPN utilizará la red Internet de manera segura para establecer la conexión con las oficinas de DHL.

- Las computadoras portátiles de DHL no deben ser conectadas a Internet a través de "conexiones permanentes" como por ejemplo las conexiones de módems de cable, DSL o líneas alquiladas, líneas en cafeterías o servicios de acceso a Internet de hoteles sin la protección de un sistema firewall personal administrado desde la central. El cliente DHL VPN no puede proteger de manera segura una computadora en dichas situaciones.
- El uso de Internet, mientras se encuentra fuera de las oficinas de DHL, se encuentra restringido a establecer una conexión con DHL a través de la facilidad de acceso remoto VPN.
- Los usuarios se comprometen a terminar la conexión de Internet (física y lógicamente) tan pronto como la conexión de acceso remoto VPN sea cerrada por el usuario en las oficinas de DHL.
- Los usuarios deben saber que existe un riesgo al conectar una computadora de DHL a redes que no son controladas por la empresa. Actualmente no existe ninguna protección contra riesgos que se originen en dichas redes. En muchas situaciones, como por ejemplo, en la red LAN interna de los hoteles o en la oficina de los clientes, existe un riesgo significativo de que personas no autorizadas puedan acceder a la computadora portátil de DHL o que la PC se vea dañada por software de naturaleza maliciosa.
- Los usuarios deben saber que el hardware no autorizado, incluyendo, a mero título enunciativo, las disqueteras, reproductores de cintas, USB-sticks, reproductores de CDROM/DVD o los adaptadores de red tales como las tarjetas de la red LAN inalámbrica, podría traer aparejados algunos riesgos. Toda la instalación o modificación del hardware se ve, por lo tanto, restringida, al personal de soporte autorizado. Esta restricción incluye toda clase de dispositivos periféricos internos y externos independientemente de la interfase (es decir USB, Tarjeta PC, etc.).
- Los usuarios no deben desconectar el protector de pantalla pre-configurado y protegido con la contraseña personal (password). El tiempo de inicio del protector de pantalla, que se encuentra configurado en 10 minutos debería reducirse toda vez que la PC sea utilizada fuera de las oficinas de DHL.



- ✗ NO SE AUTO-REENVÍE CORREOS ELECTRÓNICOS A CUENTAS DE CORREO ELECTRÓNICO DIFERENTES DE LAS DE DHL.
- ✓ ASEGURESE DE QUE SU PC SE ENCUENTRE PROTEGIDA POR UN SOFTWARE DE ANTIVIRUS Y POR PATRONES DE VIRUS ACTUALIZADOS.
- ✓ REALICE COPIAS DE SEGURIDAD (BACKUPS) DE LA INFORMACION Y ALMACENELA DE MANERA SEGURA.
- ✗ NO PERMITA QUE OTROS UTILICEN SU EQUIPO DE LA COMPAÑÍA
- ✗ NO COMPARTA ARCHIVOS EN SU PC

Incumplimiento

- La falta de cumplimiento del presente Código de Practica así como de las demás políticas de DHL podría resultar en la suspensión del acceso al sistema de DHL, en medidas disciplinarias, y hasta inclusive en la rescisión de la relación laboral y/o el inicio de acciones legales.



Declaración

Declaración

Yo, el abajofirmante,
(nombre, apellido y fecha de nacimiento) por el presente declaro haber leído la información contenida en el presente "Código de Práctica de Seguridad de la Información" emitido por DHL Information Services, s.r.o. en la versión 1.0 en vigencia a partir del 1 de Agosto de 2005 (en adelante "COP"), y manifiesto haber entendido todas sus disposiciones.

Además, declaro tener pleno conocimiento de los documentos internos a los que se hace referencia en el COP, como por ejemplo, la Política de Seguridad de la Información de DHL y el Estándar de Seguridad de la Información de Línea de Base de DHL (BISS)

Reconozco también que:

- las disposiciones del COP son de cumplimiento obligatorio y que me encuentro obligado a cumplirlas.
- la violación del COP por parte de un Empleado podría ser considerado como un incumplimiento a las obligaciones disciplinarias. En caso de incumplimiento serio de las obligaciones disciplinarias o en caso de una serie de incumplimientos no tan graves de las obligaciones disciplinarias pueden ser la causal de rescisión de la relación laboral o de la notificación de despido al empleado por parte del empleador.

En....., con fecha/...../.....

Firma del empleado

Aprobado por RRHH / Legales para Argentina, 17/06/2005



Términos, Definiciones y Referencias

Cuenta	Entidad definida para autenticar el origen de una acción. Distinguimos entre dos clases principales de cuentas, las cuentas del usuario y las cuentas técnicas. Las cuentas técnicas se refieren a la cuenta del sistema (raíz, etc.) o cuentas utilizadas como interfase de dos plataformas de IT.
Accountability/ (Seguimiento de la cuenta)	Asegura que las acciones de las cuentas sean rastreadas y asignadas exclusivamente al titular de la entidad.
Activos	Todo aquello de valor para la organización
COP	Código de Práctica de Seguridad de Información
BISS	Estándar de Seguridad de la Información de Línea de Base
Banda ancha	Un tipo de transmisión de datos en la que un solo medio (cable) puede transportar diversos canales a la vez (por ejemplo TV por cable, ADSL).
CDROM	Compact Disc Read-Only Memory
Confidencialidad	La propiedad de que la información no se encuentra disponible ni es divulgada a personas, entidades o procesos no autorizados. La Confidencialidad tiene como fin principal, proteger la información de naturaleza secreta o sensible de la divulgación no autorizada.
Credencial	Medios de validación de la identidad del usuario para acceder a un servicio o recurso de información. Una password (contraseña) es una clase de credencial común.
Criptografía	Técnicas matemáticas subyacentes al suministro de seguridad de la información, incluyendo, confidencialidad, integridad de los datos, autenticación de la entidad y autenticación del origen de datos. Las técnicas criptográficas incluyen algoritmos de encriptación, técnicas de firma digital, las funciones de algoritmos y de Código de Autenticación de Mensajes (MAC).
DVD	Digital Versatile Disk
Firewire, I-link, IEEE1394	Diversos nombres para aludir a una interfase de alta velocidad para conectar dispositivos internos a una computadora, tales como cámaras de video digital o disqueteras.
GSO	Oficina de Seguridad Global (Global Security Office)
Propietario o Titular de la Información	Ver 'Propietario'
ISM	Gerente de Seguridad de la Información. Persona responsable de brindar asesoramiento en materia de seguridad tecnológica de la información y de garantizar la coherencia en el proceso de toma de decisiones sobre seguridad de la información.
	Red de Área Local (Local Area Network)
LAN	Gerente Local de Seguridad de la Información. Brinda soporte al Gerente local IS para lograr el cumplimiento de las políticas y estándares de seguridad IS Globales de DHL.
LISM	

Software de naturaleza maliciosa	Software, parte de un código diseñado con el fin de dañar computadoras o sistemas de información o de realizar actividades no autorizadas.
Propietario	También referido como 'Propietarios Comerciales' y 'Propietarios de Información'. Personas o representantes de los directivos con aplicaciones o sistemas a su cargo, personas que otorgan acceso a la infraestructura responsables por el uso y el empleo indebido de dicha infraestructura.
PDA	Asistente Digital Personal (Personal Digital Assistant)
PIN	Numero de Identificación Personal (Personal Identification Number)
Scam	Correos electrónicos que intentan burlar a los usuarios para que entreguen dinero utilizando un esquema comercial fraudulento.
Spam	Correo electrónico no deseado (generalmente de naturaleza comercial enviado masivamente)
Tercero	Todos aquellos ajenos a la organización involucrados en operaciones o acuerdos directamente entre si.
USB	Universal Serial Bus, interfase de alta velocidad para conectar dispositivos externos a una computadora, incluyendo, el mouse, teclados, disqueteras y escáner.
USB Stick	Pequeño medio portátil para almacenar datos. Se conecta a puertos USB.
ID de Usuario	Identificador de una cuenta de usuario
Visita	Toda persona ajena al personal.
VPN	Red Privada Virtual (Virtual Private Network)
Vulnerabilidad	Debilidad de un activo o grupo de activos que pueden ser explotados por uno o mas amenazas.
WLAN	Red Inalámbrica de Área Local (Wireless Local Area Network)

Documentos Referenciados

[1] Política de Seguridad de la Información de DHL

[2] Estándar de Seguridad de la Información de Línea de Base de DHL (BISS)

Notas



Information Security

Código de Práctica



Deutsche Post  World Net

MAIL EXPRESS LOGISTICS FINANCE