Política de proveedores

Preparado para
C&A Systems

martes, 9 de septiembre de 2020

Versión: ***2.0***

Código
CA-SSI-36-Política de proveedores

Preparado por
Andrés Rocha
argarcia@casystem.com.mx

Innovando On Premises,
Desarrollando Open Source

Microsoft Gold Partner

CMMI DEV / 3 SM
Exp. 2022-12-13 / Appraisal # 5587

CMMI SVC / 3 SM
Exp. 2022-06-21 / Appraisal # 2947

1. Control de versiones

Versión	Fecha	Sección modificada	Descripción	Autor
1.0	*09/09/2020*	*Todo*	*Se creo la política*	Andrés Rocha
2.0	*27/09/2020*	*Apartado 5. Definiciones*	*Se modificó la definición de proveedor y C&A Systems*	Laura Valencia

2. Contenido

3. Objetivo del documento

El presente documento establece las políticas de seguridad de la información y seguridad aplicables a todo proveedor que brinde servicios críticos a las empresas del C&A SYSTEMS.

Las presentes políticas tienen como objetivo:

- Proteger los activos de información del C&A SYSTEMS, frente a amenazas, internas o externas, deliberadas o accidentales, para asegurar la confidencialidad, integridad y disponibilidad de la información.
- Proteger la salud y la vida del personal, que preste servicios al C&A SYSTEMS y que se encuentre dentro de las instalaciones durante la prestación de estos.

4. Alcance del documento

El documento es de cumplimiento obligatorio de todos los proveedores que brinden servicios críticos al C&A SYSTEMS, en lo que le corresponde.

ALCANCE DE LOS 5 SERVICIOS…

El proveedor que preste servicios al C&A SYSTEMS se compromete a cumplir con los lineamientos establecidos en la presente Política. En tal sentido, el proveedor se obliga a capacitar y a poner la presente Política a disposición de sus colaboradores, terceros y locadores que destaque para prestar el servicio alC&A SYSTEMS.

5. Definiciones

Proveedor: Persona física o moral que proporcione bienes o servicios a C&A Systems.

C&A Systems: persona moral constituida bajo el instrumento notarial 24495.

6. Políticas de Seguridad de la Información para proveedores

6.1. Políticas generales

1. Todo proveedor de servicios deberá velar porque su personal o terceros subcontratados que presten los servicios directamente a C&A Systems, cumplan con las políticas de seguridad de la información establecidas en el presente documento. En caso de incumplimiento, C&A Systems se reserva el derecho de solicitar al proveedor el cambio de personal, sin perjuicio del derecho de C&A Systems de resolver el contrato de prestación de servicios en los términos establecidos en elcontrato.

2. El proveedor deberá garantizar que todo el personal, que preste servicios para el C&A Systems, cuente con formación y capacitación apropiada para el desarrollo del servicio contratado, tanto a nivel específico en las materias correspondientes a la actividad asociada, como de manera transversal en materia de seguridad de la información.

3. Cualquier tipo de intercambio de información que se produzca entre C&A Systems y el proveedor se entenderá que ha sido realizado dentro del marco establecido por el contrato de prestación de servicios y la cláusula de confidencialidad de la información.

4. Todo proveedor que tenga acceso a información del C&A Systems deberá considerar que dicha información es **confidencial, y no pod**rá compartirla con ningún tercero o personal del proveedor que no esté brindando el servicio materia del contrato directamente a C&A SYSTEMS.

5. Ningún proveedor podrá utilizar la información de C&A SYSTEMS para beneficio propio o de terceros. La información a la que tenga acceso el proveedor únicamente podrá ser utilizada para los fines específicamente indicados en el contrato de prestación de servicios. Toda información proporcionada por el C&A SYSTEMS, seguirá siendo de propiedad de este último.

6. La salida de medios informáticos que contengan información confidencial o datos de carácter personal, fuera de locales en los que está ubicada la información, únicamente podrá ser autorizada por el Oficial de Seguridad de la Información del C&A SYSTEMS.

7. El proveedor debe garantizar el cumplimiento de las restricciones legales respecto del uso del material protegido por normas de propiedad intelectual.

8. Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia en los sistemas de información delC&A SYSTEMS.

9. El proveedor deberá informar al C&A SYSTEMS y esta última deberá autorizar los casos en los cuales se realice trabajos a distancia y/o uso de equipos móviles para acceder a información

del C&A SYSTEMS.

10. Todos los equipos del proveedor que requieran conectarse a la red del C&A SYSTEMS deben ser autorizados por esta última.
11. Los recursos que el C&A SYSTEMS pone a disposición del proveedor, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están exclusivamente destinados para cumplir con las obligaciones y propósito del servicio contratado. C&A SYSTEMS se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

12. Se prohíbe expresamente:

    a. El uso de recursos proporcionados por el C&A SYSTEMS para actividades no relacionadas con el propósito de servicio.
    b. Introducir por dolo o culpa inexcusable en la red del C&A SYSTEMS, cualquier tipo de malware, dispositivos lógicos, dispositivos físicos, o cualquier tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos o información del C&A SYSTEMS.
    c. Intentar obtener sin autorización explícita otros derechos o accesos distintos a los que el C&A SYSTEMS haya asignado.
    d. Intentar acceder, sin autorización explícita, a áreas restringidas del C&A SYSTEMS.
    e. Intentar distorsionar, alterar o falsificar los registros “log” de los sistemas de información del C&A SYSTEMS.
    f. Poseer, desarrollar o ejecutar programas que pudieran dañar o alterar los recursos informáticos de C&A SYSTEMS.

13. El proveedor deberá mantener una lista actualizada del personal asignado al servicio, así como también los equipos utilizados en caso convenga. Dicha relación podráser requerida por el C&A SYSTEMS en cualquier momento.

6.2. Vulnerabilidad, eventos e incidentes de seguridad de información

1. El proveedor, se compromete a reportar toda vulnerabilidad, evento o incidente que pudiera afectar la confidencialidad, integridad o disponibilidad de la información de C&A SYSTEMS.
2. Cuando el proveedor conozca de cualquier pérdida, uso no autorizado, revelación de la información, u otra circunstancia que pudiera afectar la seguridad de la información de C&A SYSTEMS, deberá comunicarlo inmediatamente mediante alguno de los siguientes medios:

    - Al personal del área de gestión tecnológica y servicios administrados de TI.
    - Al correo electrónico seguridad@casystem.com.mx

6.3. Finalización del contrato

1. El proveedor garantiza que, a la culminación del servicio o ante el pedido efectuado en cualquier momento por C&A SYSTEMS, cesará inmediatamente el uso de toda información proporcionada por esta última y entregará, cualquiera sea el soporte en que se encuentre, toda la información que obre en su poder y destruirá toda copia que haya realizado. Asimismo, entregará una confirmación por escrito de ello, la cual tendrá calidad de declaración jurada.

6.4. Políticas aplicables a proveedores que tengan acceso a equipos o sistemas de información propiedad del C&A SYSTEMS

1. El proveedor solo podrá crear "bases de datos" de forma temporal, siempre que sea estrictamente necesario para el desarrollo del servicio. Estas bases de datos temporales no deberán ser almacenadas en ninguna computadora del personal que presta los servicios contratados y deberán ser destruidas cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

2. Cada persona con acceso a la información de C&A SYSTEMS es responsable de la actividad desarrollada por su identificador de usuario y todo lo que de él derive.

3. Los usuarios no deberán utilizar ninguna cuenta de otro usuario.

4. Los proveedores de servicios de tecnología con acceso a información de C&A SYSTEMS deberán seguir las siguientes directivas en relación con la gestión de contraseñas:
   a. Seleccionar contraseñas de calidad.
   b. Cambiar contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
   c. Cambiar las contraseñas periódicamente y no reutilizar o utilizar antiguas.
   d. Cambiar las contraseñas por defecto y las temporales en su primer inicio de sesión.

5. El proveedor deberá velar por que los equipos que utilice su personal queden protegidos cuando vayan a quedar desatendidos, configurando el bloqueo automático de las pantallas en un intervalo no mayor a 10 minutos.

6. El personal del proveedor nunca deberá, sin autorización explícita, realizar pruebas para detectar y/o utilizar/explotar una debilidad o vulnerabilidad en un sistema de C&A SYSTEMS.

7. Toda persona que acceda a la información y/o sistemas del C&A SYSTEMS deberá seguir las siguientes normas:
   a. Proteger la información confidencial de toda revelación no autorizada, modificación, destrucción o uso incorrecto, sea esta accidental o no.
   b. Proteger los sistemas de información y redes de telecomunicaciones contra accesos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.

c. Contar con la autorización necesaria para obtener acceso a los sistemas de información y/o la información accedidos.

8. En los casos en que el proveedor requiera dar de baja o reasignar un equipo del C&A SYSTEMS, deberá informarlo a esta última para que se apliquen los procedimientos de TI correspondientes.

6.5. Políticas aplicables a proveedores que tengan acceso a las oficinas de C&A SYSTEMS

1. El personal del proveedor deberá portar en todo momento la tarjeta de identificación (de visitante) proporcionada por C&A SYSTEMS durante su estadía en las oficinas.

2. El personal del proveedor deberá respetar al menos las siguientes políticas de escritorios limpios:

   a. Almacenar bajo llave los documentos de papel y los medios informáticos con información de C&A SYSTEMS en mobiliario seguro cuando no están siendo utilizados.
   b. Proteger los documentos en papel de C&A SYSTEMS que se encuentren en las impresoras.
   c. Los listados con datos de carácter personal o información confidencial del C&A SYSTEMS deberán almacenarse en un lugar seguro al que únicamente tengan acceso personas autorizadas.

3. El personal del proveedor deberá mantener las puertas de acceso al edificio y a las oficinas cerradas en todo momento. Asimismo, deberá abstenerse de abrir la puerta a terceros.

4. El personal del proveedor deberá abstenerse de manipular o mover información que ha sido dejada sobre los escritorios u otras superficies. Deberá reportar que ha quedado información en la impresora al personal de C&A SYSTEMS que labora en el área adyacente a la impresora.

5. El personal del proveedor solo podrá estar presente en las áreas a las que visita, queda estrictamente prohibido desplazarse a zonas seguras o restringidas de la organización a menos que sea escoltado por personal de C&A Systems autorizado.

6.6. Seguridad en las áreas de trabajo

a) Almacenes

- Los contratistas o proveedores, asignados a la manipulación de materiales, cumplirán lo estipulado en sus propios procedimientos de trabajo diseñados para esta labor, los cuales deben observar los lineamientos generales de seguridad establecidos en el marco normativo vigente.
- Los materiales serán apilados de tal manera que:
  - No obstruya las vías de acceso o rutas de escape al almacén ni los pasadizos dentro del mismo.
  - No interfieran con la adecuada distribución de la luz artificial o natural.

- No obstruya el acceso a los tableros de distribución ni a la subestación eléctrica.

- Es obligatorio clasificar y ordenar los materiales de manera que sea fácil su ubicación, control y utilización. El tratamiento a los materiales peligrosos se detalla en la sección 5.3.
- Se deberá disponer los almacenes con estantería o anaqueles de acuerdo a las necesidades de almacenaje, se colocarán los objetos más pesados en las partes bajas de los estantes o anaqueles.
- Se efectuará una limpieza periódica de los ambientes, según su frecuencia de acceso.

b) Oficinas

En cuanto al ambiente de trabajo, se deberá tener en consideración lo siguiente:

- Deberá conservarse el orden y una adecuada distribución, de manera que las vías o rutas de escape se mantengan siempre libres de obstáculos.
- No obstruya el acceso a los equipos o salidas de emergencias.
- Acondicionar el lugar de trabajo de acuerdo con la iluminación que le brinda el lugar, la iluminación artificial deberá venir de los lados, mejorando la iluminación de la zona de trabajo.

Es importante tomar en cuenta para reducir los riesgos derivados de la electricidad, las siguientes normas de seguridad:

- Llevar un mantenimiento adecuado y regular de las instalaciones.
- Avisar a la gerencia de gestión tecnológica y servicios administrados de TI sobre cualquier irregularidad o desperfecto en los equipos o sistemas eléctricos.
- El contratista, que no haya sido contratado para esto, no deberá manipular el sistema eléctrico.

6.7. Sustancias peligrosas y ofensivas

Todo contratista que manipule sustancias peligrosas deberá estar capacitado acerca de la manipulación y uso de las sustancias que utiliza en su labor. Se exigirá que los contratistas o proveedores entreguen las hojas de seguridad de los insumos que utilizarán para el desarrollo de sus actividades.

6.8. Accidentes de trabajo

Estadísticas de accidente de trabajo

- Las estadísticas de los accidentes de trabajo que ocurran en C&A SYSTEMS

servirán para evaluar la efectividad de los programas de seguridad establecidos, así como para planificar las futuras actividades.

- C&A SYSTEMS llevará un control estadístico de los accidentes, cuasi accidentes, peligros y enfermedades ocupacionales; clasificadas por: su gravedad, frecuencia, y otras características que se consideren convenientes. Estos registros serán preservados de acuerdo con ley.

6.9. Estándares de seguridad y salud en los servicios y actividades conexas

Mantenimiento y reparación en el edificio y estructura

- Durante las obras de mantenimiento o reparación del edificio que no puedan efectuarse con seguridad desde una escalera portátil o plataforma, se elegirán cuando sea necesario andamiaje, plataformas de trabajo entablado, escaleras y demás construcciones adecuadas y seguras.
- Los contratistas o proveedores que realicen actividades de mantenimiento de las edificaciones de C&A SYSTEMS, tendrán que contar con arneses o cinturones de seguridad, resistentes y durables; cables salvavidas de longitud y resistencia adecuadas, con dispositivos que puedan ser enganchados, los cuales tendrán un cinturón de seguridad, de manera que el operario que lo utilice tenga libertad de movimiento.
- Los implementos de seguridad serán inspeccionados regularmente por el Jefe de Mantenimiento y Seguridad.

6.10. Sanciones y reclamos

Todo incumplimiento a lo definido en esta política será materia de evaluación por el Comité de Seguridad. Las decisiones sobre las sanciones se evaluarán en el Comité de Seguridad.

Las obligaciones, prohibiciones y sanciones, señaladas en este reglamento, deben ser de conocimiento de todos los colaboradores, personal propio y contratista e incorporadas en los contratos de proveedores.