Política de Seguridad de La Información Corporativa.

Resumen

Política de Seguridad de La Información Corporativa

1. Objetivo

La Política de Seguridad de la Información del Grupo 7COMm tiene como objetivo establecer los principios y lineamientos de Seguridad de la Información destinados a garantizar la confidencialidad, integridad y disponibilidad de la información, los activos, los sistemas y los recursos de procesamiento asociados a la información que posee y/o se encuentra bajo su custodia, y su cumplimiento es obligado para todos los que utilizan la información, los recursos y/u otros activos tangibles o intangibles de la empresa.

Establece reglas, estándares y mejores prácticas para asegurar la protección de la información puesta a disposición para el desempeño de las actividades profesionales y el cumplimiento de las leyes y reglamentos vigentes.

Asegúrese de que el Grupo 7COMm tenga estándares, procedimientos y controles de seguridad de la información adecuados para mitigar el riesgo de seguridad de la información y garantizar el cumplimiento de todas las leyes, reglamentos y estándares relevantes de protección de datos y privacidad.

2. Destinatarios

Esta política se aplica a todos los directores, administradores, empleados, pasantes, aprendices, colaboradores y visitantes del Grupo 7COMm y terceros involucrados, que actúan en nombre del Grupo 7COMm, como proveedores de servicios, revendedores y socios comerciales que tienen acceso a la red o utilizar el entorno de procesamiento del Grupo 7COMm y sus clientes

También se aplica a todos los activos de información y equipos informáticos, propiedad o no del Grupo 7COMm, que contengan información relevante para el negocio de la institución.

3. Responsabilidades

3.1. Comité Ejecutivo y Presidencia

3.1.1. Analizar y apoyar proyectos de Seguridad de la Información ayudando a mantener el desarrollo de la area siempre combinado con la continuidad de los negocios e intereses estratégicos del Grupo 7COMm.

3.1.2. Aprobar, observar y hacer cumplir este PSI, que incluye los principios básicos, lineamientos y responsabilidades del proceso de seguridad de la información.

3.1.3. Garantizar la implementación de esta Política, velando por el cumplimiento de sus principios y lineamientos en todas sus decisiones.

3.2. Gerentes y Líderes de Área

3.2.1. Conocer, observar y hacer cumplir los estándares de PSI, así como sus buenas prácticas, los procedimientos involucrados y orientar a los miembros del equipo en su trabajo diario.

3.2.2. Informar a los responsables de Tecnologías de la Información y/o Seguridad de la Información a través de correo electrónico, canales de denuncia o personalmente sobre todos y cada uno de los eventos, conductas o incidentes que comprometan la seguridad de la información.

3.3. Sector de Tecnología de la Información

3.3.1. El Sector de Tecnologías de la Información está subordinado a la Gobernanza de TI.

3.3.2. Programar, ejecutar y cumplir la presente política, actuando en su desarrollo y en la difusión permanente y sistemática de su contenido a las partes interesadas.

3.3.3. Revisar y actualizar anualmente la política de seguridad, adaptándola a la realidad tecnológica.

3.3.4. Registrar y manejar incidentes de seguridad y cambios en el entorno a través de los recursos computacionales disponibles de acuerdo con los procedimientos operativos actuales.

3.4. Comité Corporativo

3.4.1. Leer, comprender y cumplir en su totalidad los términos de la Política General de Seguridad de la Información, así como las demás normas y procedimientos para seguridad aplicables.

3.4.2. Notificar a la Gerencia de Tecnologías de la Información cualquier evento que viole

esta política o pueda poner en riesgo la seguridad de la información o los recursos computacionales del Grupo 7COMm.

3.4.3. Comprender el papel de la seguridad de la información en sus actividades diarias y participar en programas de concientización.

3.5 Proveedores de servicios, revendedores, socios comerciales y visitantes

3.5.1. Comprender, respetar y seguir la PSI puesta a su disposición por Grupo 7COMm desde el momento en que tenga acceso a la red o utilice el entorno de procesamiento del Grupo 7COMm y sus clientes.

4. Pautas

4.1. Acceso a la red corporativa

Grupo 7COMm proporciona a sus usuarios autorizados cuentas de acceso que permiten el uso de activos de información, sistemas de información y recursos computacionales, como la red corporativa.

4.1.1. Se establece que la norma de gestión de acceso IAM, NOR SEG 001/21, es complementaria a esta política por contener detalles del proceso.

4.1.2. Cada cuenta de acceso es personal del usuario en quien se delegó e intransferible.

4.1.3. El usuario es totalmente responsable de su uso, respondiendo por cualquier violación o acto irregular/ilícito, incluso si es ejercido por otra persona y/u organización en posesión de su cuenta de acceso.

4.1.4. Para garantizar la seguridad de la información, Grupo 7COMm practica el bloqueo de acceso a la red y cuentas de correo electrónico en las siguientes situaciones: solicitudes de emergencia, ataques o riesgo cibernético y resignación

4.1.5. Está prohibido el uso de notebooks, computadoras, tabletas que sean privadas en la red corporativa que no sigan las reglas BYOD (Bring Your Own Device).

4.1.6. Los equipos personales de los visitantes, proveedores y prestadores de servicios deben conectarse a la red de visitantes (WIFI – Guest).

4.1.7. Se prohíbe la instalación de cualquier equipo en la red sin la debida autorización de la gerencia de tecnología de la información.

4.1.8. No anote ni registre las claves de acceso en ningún lugar, excepto en las herramientas proporcionadas oficialmente por Grupo 7COMm

4.2. Contraseñas de acceso

Cada contraseña de acceso es personal del usuario, delegada e intransferible. De esta forma, el usuario es totalmente responsable de su uso, respondiendo por cualquier violación o acto irregular/ilícito, incluso si lo ejerce otra persona y/u organización en posesión de su contraseña de acceso.

Los usuarios deben tomar medidas de precaución para garantizar el acceso seguro a los activos y servicios de información, que incluyen:

4.2.1. Las contraseñas tienen una validez de 90 (noventa) días. Después de este período, los sistemas solicitarán automáticamente el cambio de contraseña.

4.2.1. Las contraseñas asociadas a cuentas con privilegios no administrativos estarán compuestas con una cantidad mínima de 8 (ocho) dígitos, combinando letras mayúsculas, minúsculas, números y caracteres especiales; la nueva contraseña no puede ser la misma que ninguna de las últimas 10 contraseñas utilizadas.

4.2.2. Después de 05 (cinco) intentos de acceso con contraseñas no válidas, el usuario será bloqueado, permaneciendo por lo menos 30 (treinta) minutos;

4.2.3. Al unirse al comité corporativo del Grupo 7COMm, todos los usuarios y terceros usuarios reciben un “nombre de usuario” y una “contraseña temporaria” para iniciar sus actividades. La contraseña temporaria deberá ser cambiada en el primer acceso, siendo compuesta dentro de los estándares mencionados en esta política.

4.2.4. Cualquier uso no autorizado o intento de uso no autorizado de credenciales y contraseñas para acceder a activos/servicios de información o recursos computacionales será

tratado como un incidente de seguridad de la información, con análisis de la infracción por parte del área responsable de Seguridad de la Información y aplicación de sanciones previstas en la Política de Seguridad de la Información, según la gravedad de la infracción. Si la cuenta del empleado se ve involucrada en un posible incidente, la cuenta puede ser bloqueada inmediatamente.

4.2.5. Recomendaciones de contraseña de acceso: al crear una nueva contraseña, los usuarios deben prestar atención a las siguientes recomendaciones:

4.2.5.1. No utilice ninguna parte de su credencial en la composición de la contraseña;

4.2.5.2. No utilice ninguno de sus nombres, apellidos, nombres de familiares, compañeros de trabajo o información sobre usted que sea fácil de obtener, como, por ejemplo, placa del automóvil, fecha de nacimiento o dirección;

4.2.5.3. No utilice repetición o secuencia de caracteres, números o letras;

4.2.5.4. Cualquier parte o variación del nombre del Grupo 7COMm;

4.2.5.5. Cualquier variación de los elementos descritos anteriormente, como duplicación o escritura inversa

4.3. Uso de Archivos, Directorios y Almacenamiento de Datos

4.3.1. Todas las solicitudes de acceso a los datos deben ser procesadas de acuerdo con el procedimiento actual de gestión y acceso del Grupo 7COMm y los plazos especificados por la legislación pertinente.

4.3.2. Esta política aborda las reglas básicas para el uso protegido y apropiado de los datos del Grupo 7COMm, los detalles y reglas más técnicas y específicas se abordarán en el estándar de gestión de la información.

4.3.3. Las concesiones, revisiones y exclusiones deberán basarse en conceptos de autoridad, autenticidad y privilegios mínimos de acceso, teniendo cada uno acceso únicamente a la información que sea necesaria para el desarrollo de sus actividades profesionales.

4.3.4. El responsable de cada sistema/plataforma deberá autorizar el acceso a los datos, además de realizar revisiones periódicas.

4.3.5. Si TI identifica un riesgo de seguridad de la información, puede cuestionar la solicitud de acceso y proponer una sugerencia de cambio.

4.3.6. Seguridad de la Información podrá auditar el acceso a la información y su uso adecuado en cualquier momento, aplicar las sanciones de Nivel 1 que correspondan, orientar y realizar las correcciones necesarias para cumplir con las normas de la política de seguridad de la información vigente. En caso de cualquier infracción, la dirección de los involucrados debe ser informada vía correo electrónico.

4.3.7. Siempre que exista la necesidad de transferir un usuario o un tercero a otro departamento o función y exista la necesidad de revisar los accesos existentes, el ex gerente debe registrar una llamada para bloquear los accesos previamente otorgados.

4.3.8. Los datos de propiedad del Grupo 7COMm, o no, deberán ser almacenados exclusivamente en sus servidores y plataforma corporativa en la nube y en servidores de archivos. Los datos impresos deben archivarse correctamente en lugares seguros.

4.3.9. El acceso a los archivos y directorios se realiza a través de compartir en la red, respetando las reglas de gestión de acceso por perfil a través de cuentas de red, sin embargo, es responsabilidad de los jefes de área abrir un ticket con TI para solicitar, revisar y acceder revocación.

4.3.10. Está prohibido el uso de medios externos como: Pendrives, HDs y CDs Externos para copias privadas de datos de trabajo.

4.3.11. El secreto de la información es responsabilidad de todos los destinatarios y está prohibido el uso no autorizado de la información del Grupo 7COMm.

4.3.12. La confidencialidad y privacidad de la información debe ser una prioridad como se indica en la política de secreto y privacidad a la que se hace referencia en el punto 4.5 de este documento.

4.4. Gestión de activos

Esta política tiene como objetivo establecer pautas para el uso aceptable, entendido como seguro, de los activos de información del Grupo 7COMm, por parte de sus usuarios autorizados.

Todo usuario debe observar las siguientes disposiciones con respecto al uso de equipos de propiedad del Grupo 7COMm:

4.4.1. El Grupo 7COMm proporciona a sus usuarios equipos exclusivamente para el desempeño de sus actividades profesionales.

Los equipos puestos a disposición con la finalidad específica de permitir a los usuarios el desarrollo de sus actividades profesionales son propiedad del Grupo 7COMm, quedando expresamente prohibido su uso para fines particulares;

4.4.2. La modificación y/o mantenimiento de cualquier equipo de propiedad del Grupo 7COMm es una atribución específica del departamento de infraestructura interna del Grupo 7COMm que, a su exclusivo criterio, podrá ser delegada formalmente para otro responsable. Se prohíbe expresamente a otros usuarios realizar cualquier tipo de mantenimiento o modificación en el equipo;

4.4.3. Los equipos del grupo 7COMm deben utilizarse con cuidado para garantizar su conservación y correcto funcionamiento.

4.4.4. Las computadoras de escritorio (desktops) o las computadoras móviles (notebooks) deben ser bloqueadas al final de la jornada laboral o cuando el usuario esté ausente.

4.4.5. Para la liberación o préstamo de activos del Grupo 7COMm, es necesario firmar el Contrato de Préstamo de Equipos - Notebook y Periféricos y/o Término de Recibo y Responsabilidad - Notebook y Periféricos, y esto sólo ocurrirá después de la firma de los documentos

4.4.6. Al término de la prestación de los servicios y/o relación contractual, los equipos puestos a disposición para el desempeño de actividades profesionales deberán ser devueltos en un adecuado estado de conservación cuando el usuario resigne o finalice la relación con el Grupo 7COMm.

4.4.7. A su exclusivo criterio, el Grupo 7COMm podrá permitir el uso de equipos privados para el desempeño de actividades profesionales, los cuales deberán ser evaluados técnica-

mente por el departamento de tecnología de la información, asegurando que se encuentren dentro de los estándares mínimos de seguridad.

4.4.8. No se permite la conexión de dispositivos de red, wifi o telefonía a la red del Grupo 7COMm sin autorización del sector de las tecnologías de la información. Estos equipos por seguridad tiene una instalación normalizada y el incumplimiento de esta norma se considera grave.

4.4.9. El Grupo 7COMm podrá, a su sola discreción, proporcionar a sus usuarios dispositivos móviles o dispositivos con capacidad de almacenamiento removible para realizar actividades profesionales, sujeto al cumplimiento de los lineamientos de la norma general de almacenamiento de datos.

4.4.10. No será admisible, en ningún caso, la reutilización de páginas ya impresas y que contengan información clasificada como confidencial, las cuales deberán ser desechadas de acuerdo con los procedimientos adoptados por el Grupo 7COMm.

4.4.11. El Grupo 7COMm podrá, a su sola discreción, proporcionar certificados digitales a usuarios que realicen actividades profesionales específicas, siendo cada receptor responsable de su uso adecuado y aceptable, observando los lineamientos del estándar de identificación digital.

4.4.12. El uso de equipos de impresión y reprografía (fotocopiadoras) debe hacerse exclusivamente para la impresión/reproducción de documentos que sean de interés del Grupo 7COMm o que estén relacionados con el desempeño de las actividades profesionales del usuario.

4.4.13. En los casos de acceso no autorizado, extravío, sustracción o hurto de los dispositivos informáticos pertenecientes al Grupo 7COMm, el usuario responsable deberá comunicar inmediatamente la incidencia al departamento de tecnologías de la información.

4.5 Privacidad y Confidencialidad de la Información

4.5.1. Todos los empleados que tengan acceso a la información del Grupo 7COMm o bajo la custodia de la empresa -estratégica, personal, sensible o no- no pueden utilizarlos para fines personales o revelarlos a personas no autorizadas. Las restricciones incluyen el uso de datos en conferencias, presentaciones, publicaciones o cualquier otra divulgación al pú-

blico externo sin la aprobación previa de del comité de la empresa.
4.5.2. Para garantizar la integridad y fiabilidad de los datos, el Grupo 7COMm confía en el uso de tecnologías de virtualización integradas en el almacenamiento en la nube manteniendo su entorno seguro en caso de desastres.

4.5.3. El Grupo 7COMm trata datos personales para fines específicos y de acuerdo con las bases legales previstas en la LGPD.

4.5.4. Los datos personales son información relacionada con una persona viva que es o puede ser identificada a partir de los datos o los datos junto con otra información que está o es probable que esté en posesión del Grupo 7COMm. Todos los destinatarios de esta Política que traten datos deben conocer y seguir las pautas de la Política de Privacidad del Grupo 7COMm, asegurando la confidencialidad y privacidad de los datos de acuerdo con la legislación vigente.

4.6. Copia de seguridad y restauración

4.6.1. Para garantizar la integridad y confiabilidad de los datos, el Grupo 7COMm se basa en el uso de tecnologías de virtualización integradas con el almacenamiento en la nube, manteniendo su entorno seguro en caso de desastres.

4.6.2. El sector de tecnología de la información realiza periódicamente pruebas de restauración para garantizar la disponibilidad en caso de desastre. Los detalles técnicos se detallan en el estándar de gestión de copias de seguridad que complementa esta política.

4.6.3. Las restauraciones se pueden solicitar a través de un ticket y se seguirá su SLA de acuerdo con la política de gestión del servicio.

4.6.4. La Política de backup no contempla cópia de seguridad de la información almacenada en estaciones de trabajo (Desktop/Notebook), por lo que es necesario que los usuarios almacenen la información únicamente en servidores o recursos ofrecidos por el Grupo 7COMm.

4.7. Acceso remoto

El Grupo 7COMm brinda acceso VPN a usuarios y usuarios de terceros que brindan servicios remotos para garantizar una conexión segura a su red corporativa.

4.7.1. Solo los equipos validados y configurados por el equipo de TI pueden acceder a la VPN.

4.7.2. Solo el equipo de Infraestructura interna del Grupo 7COMm está autorizado para realizar acceso remoto a computadoras de escritorio, portátiles, dispositivos y servidores con fines de mantenimiento y monitoreo. Si surge alguna necesidad, el gerente del empleado debe abrir un ticket sujeto a los plazos del SLA del servicio.

4.7.3. El acceso de usuarios remotos y de terceros a los activos/servicios de información o recursos computacionales del Grupo 7COMm solo se puede otorgar después de que el acuerdo de confidencialidad entre las partes entre en vigencia y debe ser monitoreado por la infraestructura interna del Grupo 7COMm. La concesión del acceso deberá limitarse al tiempo estimado necesario para la actividad del tercero o prestador del servicio. Se otorgarán privilegios mínimos de acceso para la ejecución de actividades.

4.7.4. El usuario tercero, así como la empresa donde trabaja, serán los únicos responsables de cualquier acción realizada con sus credenciales de acceso remoto, incluida cualquier actividad no autorizada realizada por otras partes en posesión de sus credenciales de acceso remoto.

4.7.5. Durante el monitoreo de acceso remoto a sus activos/servicios de información o recursos computacionales, Grupo 7COMm se reserva el derecho, sin previo aviso , de interceptar, registrar, grabar, leer, copiar y divulgar por, o a, personas autorizadas para fines oficiales, incluidas las investigaciones criminales, toda la información transmitida, ya sea que se origine en su red interna y esté destinada a redes externas o de otro modo.

4.8 Control de acceso físico

El acceso al ambiente controlado debe realizarse a través de una credencial única, personal e identificable y no puede ser entregada a otra persona;

Este tema tiene como objetivo formalizar las pautas para el acceso físico al Centro de Datos del Grupo 7COMm. El control de acceso al resto de locales se realizará de acuerdo con la especificidad de cada zona a visitar, donde se observarán los criterios establecidos por los responsables de los mismos.

Se deben cumplir las siguientes pautas para entornos de acceso controlado:

4.8.1. Solo se permite el acceso al Centro de Datos al equipo de Infraestructura de TI, Seguridad de la Información u otras personas supervisadas.

4.8.2. En las auditorías internas o externas, los auditores siempre deben ingresar al Centro de Datos acompañados por al menos un miembro del equipo del Grupo 7COMm.

4.8.3. En el caso de servicios de terceros a realizar dentro del Centro de Datos, se requiere seguimiento y aprobación por parte del área de TI y Seguridad de la Información.

4.8.4. Todo acceso al Centro de Datos deberá estar registrado en su propio sistema de control de acceso y será permitido mediante el uso de una tarjeta de acercamiento.

4.8.5. Los registros de acceso al Centro de Datos deben almacenarse en un lugar seguro y deben mantenerse en el historial por lo menos 1 (un) año.

4.8.6. En entornos de acceso controlado, está prohibido el uso de cámaras, estén o no conectadas al teléfono inteligente, excepto en situaciones inherentes a la rutina de trabajo y/o bajo autorización informática.

4.9. Del Uso Aceptable de Internet Corporativo

Este tiene como objetivo formalizar las pautas generales para el uso de Internet, Correo Electrónico, Redes Sociales y herramientas de mensajería instantánea en las instalaciones del Grupo 7COMm.

4.9.1. Internet debe ser utilizado por los usuarios y terceros usuarios, para actividades relacionadas con el trabajo y estar disponible de acuerdo con la necesidad correspondiente al perfil funcional de cada usuario, con el objetivo de satisfacer las necesidades de las respectivas áreas;

4.9.2. En los casos en que el acceso sea necesario para otros fines, se podrá poner a disposición internet con la debida autorización del responsable inmediato, siendo controlado y vigilado dicho acceso;

4.9.3. El acceso a Internet para personas no afiliadas al Grupo 7COMm puede estar disponible en un entorno tecnológico separado (red de visitantes), controlado y monitoreado,

ya sea a través de medios móviles (wi-fi) o fijos;

4.9.4. El otorgamiento de acceso a la red de visitantes debe estar asociado al conocimiento de las normas internas de uso de la red.

4.9.5. El Grupo 7COMm busca priorizar el cumplimiento de las leyes vigentes, para asegurar el cumplimiento el Grupo 7COMm adopta algunas medidas de monitoreo y bloqueo, actuando preventivamente, mejorando la seguridad, alineando sus objetivos de negocio;

Los siguientes elementos están sujetos a monitoreo, bloqueo y sanciones si se realizan con los activos del Grupo 7COMm:

1. Navegación excesiva en sitios que no son estratégicos para el negocio del Grupo 7COMm

2. Navegación en sitios que permitan o fomenten la descarga y/o distribución de sitios pirateados,

3. Navegar por sitios web inapropiados.

4. Navegar por sitios que promuevan los juegos de azar.

5. Divulgación o propagación de difamación, perjuicio o conducta fraudulenta.

4.9.6. El acceso a redes sociales (ej.: facebook, linkedin, etc.) o a sitios que cuenten con audio y/o video (ej.: radios, tv online, youtube, etc.) son controlados y puestos a disposición únicamente de áreas que necesitan utilizar estos recursos en sus actividades laborales. Las solicitudes de liberación de estos sitios deben hacerse mediante la apertura de un ticket, lo cual debe ser autorizado por el gerente inmediato y archivado para efectos de auditoría;

4.9.7. No se permiten software con características peer-to-peer (P2P), tales como Emule, Kazaa, Morpheus, Torrent y similares, por lo que deben ser restringidos por el área técnica de Seguridad de la Información y monitoreado el acceso de los usuarios, a fin de garantizar la seguridad y el correcto uso de internet;

4.9.8. Está prohibido proporcionar o divulgar en Internet (sitios de registro, grupos de discusión, redes sociales, entre otros) información del Grupo 7COMm que sea clasificada como interna, reservada o confidencial.

4.9.9. Cualquier información que se acceda, transmita, reciba o produzca en internet dentro

de la empresa podrá ser auditada sin previo aviso. El Grupo 7COMm se reserva el derecho de monitorear y realizar auditorías constantes de acceso a los sitios web visitados por los usuarios y usuarios terceros dentro del cumplimiento legal.

4.9.10. Los destinatarios de esta PSI serán responsables de cualquier acto o infracción causado por imprudencia o mala práctica que pueda comprometer la seguridad de la información a través del uso de Internet.

4.10 Uso del Correo Electrónico Corporativo

El Grupo 7COMm presta el servicio de correo electrónico exclusivamente para el desempeño de sus actividades profesionales a los usuarios y usuarios terceros autorizados;

4.10.1. No está permitido con fines laborales, el uso de cualquier servicio de correo electrónico, distinto al que oficialmente brinda el Grupo 7COMm;

4.10.2. No está permitido utilizar el servicio de correo electrónico a título personal o para fines que no sean de interés del Grupo 7COMm;

4.10.3. No está permitido enviar información clasificada como USO INTERNO o CONFIDENCIAL a direcciones electrónicas que no sean del dominio corporativo del Grupo 7COMm, salvo autorización expresa;

4.10.4. Durante el monitoreo, el Grupo 7COMm se reserva el derecho, sin previo aviso o advertencia, de monitorear, interceptar, grabar, leer, bloquear, redirigir, retransmitir, copiar y divulgar por o a personas autorizadas para fines oficiales, incluidas las investigaciones criminales. , todos los mensajes enviados o recibidos por los usuarios a través de su servicio de correo electrónico sin previo aviso;

4.11 Mensajería

4.11.1. El Grupo 7COMm pone a disposición de toda su organización Microsoft Teams y adopta esta aplicación como estándar. Queda expresamente prohibido utilizar cualquier otro servicio de mensajería que no sea el estándar del Grupo 7COMm para la comunicación o el intercambio de datos. Excepto cuando a petición expresa de un cliente;

4.12 Desarrollo seguro

Estas pautas tienen como objetivo garantizar que la seguridad de la información sea una parte integral de todo el ciclo de vida de los sistemas de información, estableciendo pautas y requerimientos para el desarrollo y mantenimiento de los sistemas de información, proporcionando regulaciones para el desarrollo de software seguro dentro del Grupo 7COMm.

En cuanto al almacenamiento de datos, no se deben utilizar medios de almacenamiento que no tengan acceso de lectura y escritura restringido por contraseña, además, se deben almacenar preferentemente encriptados.

4.12.1. Respecto al acceso a la base de datos:

1. Las aplicaciones no deben tener acceso a una base de datos utilizando un inicio de sesión de usuario con permisos de raíz.

2. Las aplicaciones no deben tener acceso a una base de datos utilizando un inicio de sesión de usuario con permisos para ejecutar comandos en lenguaje de definición de datos (DDL).

3. No se debe dar acceso a las aplicaciones a una base de datos utilizando un inicio de sesión de usuario con permisos más allá de los estrictamente necesarios para su funcionamiento.

4. Las reglas anteriores podrán ser modificadas de acuerdo a las necesidades de cada cliente y deberán ser debidamente justificadas.

4.12.2. Respecto al uso de contraseñas:

1. No debe permitirse la creación de contraseñas que no sigan los estándares establecidos en las normas de gestión de acceso del Grupo 7COMm.

2. No se debe utilizar el almacenamiento de contraseñas en el código fuente.

3. Los entornos de homologación y producción no pueden tener las mismas contraseñas que los entornos de desarrollo y prueba.

4.12.3. Sobre la autorización y autenticación de usuarios

1. Las contraseñas no deben almacenarse en texto sin formato sin usar un algoritmo seguro de hash y salt.

2. Siempre que sea posible, se debe utilizar la autenticación AD o LDAP.

4.12.4. Autenticación en Sistemas Web:

1. Dado que HTTP es un protocolo sin estado, que utiliza cookies para mantener las sesiones de los usuarios, es necesario garantizar tanto la seguridad del intercambio de credenciales como la seguridad de las demás páginas a las que acceden los usuarios de los sistemas web. El protocolo HTTPS pretende contribuir a garantizar esta seguridad.

2. Por lo tanto, HTTPS debe usarse en todas las pantallas del sistema.

4.12.5. Ataques y Defensa:

1. Se deben prevenir los ataques de inyección SQL.

2. No se deben crear SQLs concatenando parámetros textuales de fuentes no seguras, como parámetros rellenados por el usuario o incluso almacenados en la base de datos.

3. Debe restringir los permisos de acceso a la base de datos para el usuario de la aplicación.

4. Siempre que sea posible, pase parámetros en comandos SQL (DML o DDL) usando sentencias preparadas. Las consultas que no se pueden parametrizar deben recibir un tratamiento especial, como escapes o codificación hexadecimal.

5. Se deben prevenir los ataques de inyección de HTML y Javascript.

6. Se deben prevenir los ataques de secuencias de comandos entre sitios (XSS).

7. Deben prevenirse los ataques de autenticación rota y administración de sesiones.
8. Los sistemas en el área de Producto deben someterse a herramientas de prueba de penetración.

4.12.6. Respecto a las pruebas

1. Deberán realizarse pruebas de seguridad en cada versión del software que modifique su estructura (pantallas de inicio de sesión, servicios no autenticados, nuevos formularios con interacción del usuario, etc.) cuando corresponda, a definir por el responsable técnico de la aplicación.

2. Deberá asegurarse, mediante pruebas automatizadas, que los servicios y datos confidenciales están protegidos y disponibles únicamente para los usuarios que poseen la información.

3. Debe diseñarse una política de pruebas, automatizadas o no, para asegurar la no vulnerabilidad a los principales ataques conocidos a los sistemas.

4. Deben definirse escenarios de prueba destinados a garantizar los requerimientos no funcionales del software, realizados preferentemente por un equipo de pruebas diferente al equipo de desarrollo del software, para evitar vicios.

Se deben definir escenarios de prueba, principalmente en los aspectos de seguridad, para casos de actualizaciones de la arquitectura del sistema (servidores de aplicaciones, bases de datos, versiones de navegadores, versiones de sistemas operativos, etc.).

4.12.7. Acceso al repositorio origen y reglas de negocio

1. Para cada proyecto hay un área específica en nuestros repositorios y el acceso tanto a las fuentes como a las reglas de negocio está permitido solo a los colaboradores que de alguna manera están involucrados con el proyecto.

2. El acceso se controla mediante usuario y contraseña definidos en el Active Directory corporativo a cargo del área de seguridad e infraestructura.

3. Se permite el acceso a los repositorios, mediante solicitud formal del líder del equipo responsable, cuando un usuario inicia en el proyecto.

4. Los accesos se retiran inmediatamente cuando el usuario deja la empresa, se va de licencia, abandona el proyecto o es reasignado.

5. Al final del proyecto, se retiran todos los accesos;

6. Además del mantenimiento diario, se realiza una evaluación trimestral con los líderes y se verifica si los usuarios aún deben continuar con los accesos existentes, de lo contrario, se retiran los accesos.

5. Sanciones

Al tomar conocimiento de esta Política, todos los destinatarios son responsables de cumplir con sus disposiciones y de asegurarse de que los terceros en su relación estén informados sobre su contenido.

Las violaciones, incluso por omisión o intento fallido de esta Política, sus reglas y procedimientos publicados pueden resultar en sanciones como las que se describen a continuación:

Nivel 1 – Las actuaciones de las personas que puedan generar incidentes cotidianos y de baja gravedad serán tratadas con medidas informativas y correctoras, tales como:

- Advertencia verbal;

- Notificación formal.

Nivel 2 – Acciones que pueden causar incidentes graves, pero con daño bajo, pueden generar sanciones administrativas, tales como:

- Suspensión no pagada;

- Cancelación del contrato principal firmado.

Nivel 3 – Acciones que pueden causar incidentes graves y pérdidas elevadas, pueden conducir a infracciones legales, tales como, pero no limitadas a:

- Aplicación de las sanciones laborales previstas en la legislación vigente, incluido el despido por justa causa;

- Procedimientos civiles o penales;
- Indemnización de daños causados al Grupo 7COMm.

La existencia de infracciones recurrentes y continuas hace que las incidencias sean graves.

En las infracciones que tengan relación con actividades delictivas o que puedan causar daños, el infractor será responsable de los daños, con la aplicación de las medidas legales correspondientes.

6. Glosario Técnico

– BYOD:

BYOD son las siglas de Bring Your Own Device, en español “traiga su propio dispositivo”.

– Criptografia:

la criptografia en ciberseguridad es la conversión de datos de un formato legible a un formato codificado.

– Centro de Datos:

Es un entorno diseñado para albergar servidores y otros activos corporativos tales como sistemas de almacenamiento de datos (almacenamientos) y activos de red (conmutadores, enrutadores) con seguridad y control. El objetivo principal de un Centro de Datos es garantizar la disponibilidad de equipos que almacenan información corporativa y que alojan sistemas corporativos que son cruciales para el negocio de la Institución.

– Homologación:

El entorno de homologación es un entorno donde el cliente debe probar las funcionalidades del sistema que luego serán puestas en producción o, en caso de problemas, será rehecho, en caso de que el cliente no lo apruebe.

– LGPD:

Ley General de Protección de Datos.

– Backup:

El término backup significa “copia de seguridad”, y corresponde a la creación y almacenamiento de copias de archivos digitales importantes, de manera que sea posible restaurarlos en caso de pérdida de los archivos originales.

– Restaurar:

Restaurar es la acción de recuperar datos almacenados en un dispositivo determinado durante la rutina de backup, asegurando que toda la información registrada esté intacta.

– Servidor:

Servidor es un equipo que centraliza servicios, ofreciéndolos a otros equipos de su red. Dichos servicios pueden ser de diferente naturaleza, tales como correo electrónico, sitio web, almacenamiento de archivos, entre otros.

– SLA:

El significado del acrónimo SLA es “Service Level Agreement”, en español, “Acuerdo de Nivel de Servicio”, “Contrato de Nivel de Servicio” o “Garantía de Nivel de Servicio”.

– VPN:

VPN significa “Red Privada Virtual”, es decir, “Red Privada Virtual”. Como su nombre lo indica, es una red privada de usuario que brinda más seguridad al navegar, ya que cuenta con mejor encriptación, protegiendo tus datos.