Normativa de Seguridad de la Información

Este documento impreso estará vigente siempre que la edición que en él figura coincida con la del archivo informático correspondiente colocado en la carpeta de dominio interno de la Empresa.

ÍNDICE

ÍNDICE

1 OBJETO

La continua evolución tecnológica que se está experimentado deriva a la creciente digitalización de las entidades, con una gestión considerable de volúmenes de datos, herramientas específicas y gran variedad de dispositivos, conlleva que exista un sistema informático complejo donde la seguridad debe estar garantizada en todo momento. Los usuarios deben ser conscientes de la importancia de dicha seguridad y disponer de unas normas de obligado cumplimiento respecto al uso de los sistemas informáticos.

Por ello, con el fin de garantizar la correcta gestión del sistema, Aula Abierta acuerda aprobar las siguientes normas de utilización de los sistemas de información para garantizar el buen uso de los medios técnicos puestos a disposición de los usuarios.

2 ALCANCE

Esta Normativa es aplicable a todo el ámbito de actuación de Aula Abierta, dentro del alcance de la adecuación al Esquema Nacional de Seguridad, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información.

El alcance son los Sistemas de Información **que soportan la prestación de los servicios de gestión integral de instalaciones deportivas y consultoría deportiva, formación en idiomas en modalidad presencial y online, gestión de licitaciones y servicios públicos, y gestión de actividades extraescolares y servicios educativos complementarios.**

La presente Normativa es de aplicación y de obligado cumplimiento para todo el personal que,de manera permanente o eventual, preste sus servicios en Aula Abierta, incluyendo el personal deproveedores externos, cuando sean usuarios de los Sistemas de Información de Aula Abierta.

En el ámbito de la presente normativa, se entiende por usuario cualquier usuario perteneciente o ajeno a Aula Abierta, así como personal de organizaciones privadas externas, entidadescolaboradoras o cualquier otro con algún tipo de vinculación con Aula Abierta que utilice o posea acceso a los Sistemas de Información de Aula Abierta.

3 VIGENCIA

La presente Normativa de Seguridad de la Información ha sido aprobada por Aula Abierta, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que Aula Abierta pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

4 REVISIÓN Y EVALUACIÓN

La gestión de esta Normativa de Seguridad de la Información corresponde al Comité de Seguridad de la Información, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.
- Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad revisará la presente Normativa, que se someterá, de haber modificaciones, a aprobación.
- La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.
- Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5 UTILIZACIÓN DEL EQUIPAMIENTO INFORMÁTICO Y DE COMUNICACIONES

Aula Abierta facilita a los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos que Aula Abierta pone a disposición de los usuarios deben utilizarse para el **desarrollo de las funciones encomendadas, es decir, para fines profesionales**. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.

En general, el ordenador personal (PC) será el recurso informático que permitirá el acceso delos usuarios a los Sistemas de Información y servicios informáticos de Aula Abierta, constituyendoun elemento muy importante en la cadena de seguridad de los sistemas de información, razón por la que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.

Este apartado concierne específicamente a todos los equipos facilitados por Aula Abierta para su utilización por parte de los usuarios, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidades de acceso a los Sistemas de Información de la organización.

6 NORMAS GENERALES

- Los ordenadores deberán utilizarse únicamente para fines corporativos y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.

- Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa del Responsable de Seguridad.

- Salvo autorización expresa del Responsable de Seguridad, los usuarios no tendrán privilegio de administración sobre los equipos.

- Los ordenadores de la organización deberán mantener actualizados los parches de seguridad de todos los programas que tengan instalados. Se deberá prestar especial atención a la correcta actualización, configuración y funcionamiento de los programas antivirus y cortafuegos.

- Los usuarios deberán notificar al responsable de Seguridad de Aula Abierta, a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo. El conocimiento y la no notificación de una incidencia por parte de un usuario serán considerados como una falta contra la seguridad de la información de Aula Abierta.

- El usuario debe ser consciente de las amenazas provocadas por malwares. Muchos virus y troyanos requieren la participación de los usuarios para propagarse a través de memorias USB, mensajes de correo electrónico o instalación de programas descargados

desde Internet. Es imprescindible, por tanto, vigilar el uso responsable de los equipos para reducir este riesgo.

- El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata al Responsable de Seguridad, con el objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por Aula Abierta estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente a la unidad responsable cuando finalice su vinculación con dicho puesto o función.

7 USOS ESPECÍFICAMENTE PROHIBIDOS

Están terminantemente prohibidos los siguientes comportamientos:

- Utilización de cualquier tipo de software dañino.
- Utilización de programas que, por su naturaleza, hagan un uso abusivo de la red.
- Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por Aula Abierta, sin la previa autorización del Responsable de Seguridad.
- Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por Aula Abierta.
- Utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, salvo autorización y solicitud expresa del Responsable de Seguridad.
- Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.
- Intentar distorsionar o falsear los registros LOG del sistema.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de Aula Abierta.
- Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la empresa, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.

8 NORMAS ESPECÍFICAS PARA EQUIPOS PORTÁTILES

- Los equipos portátiles están asignados, controlados y registrados por el Responsable de Seguridad (número, asignación, terminal)
- Este tipo de dispositivos estará bajo la custodia del usuario que los utilice, quién deberá adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.
- La sustracción de estos equipos se ha de poner inmediatamente en conocimiento del Responsable de Seguridad para la adopción de las medidas que correspondan y a efectos de baja en el inventario.
- Los equipos portátiles deberán utilizarse únicamente para fines empresariales, especialmente cuando se usen fuera de las instalaciones de Aula Abierta.
- Los equipos portátiles serán transportados fuera de las instalaciones de Aula Abierta en una mochila cerrada con candado.
- Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas a Aula Abierta, no autorizadas para ello.
- Los usuarios de equipos portátiles no deberán interrumpir los procesos de actualización de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad que hayan sido definidos y planificados por el Responsable de Seguridad.

9 IDENTIFICACIÓN Y AUTENTICACIÓN

- Los usuarios dispondrán de un código de usuario y una contraseña, para el acceso a los Sistemas de Información de Aula Abierta, y son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado. El código de usuario es único para cada persona en la organización, intransferible e independiente del PC o terminal desde el que se realiza el acceso.
- Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso o tarjeta criptográfica a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros.

- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.
- Ante una baja o ausencia temporal del usuario, el Responsable del Departamento podrá solicitar al Responsable del Sistema la cesión de la clave a la persona por él designada, cuando el usuario ausente regrese deberá cambiar nuevamente sus credenciales.
- Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar al Responsable de Seguridad a través de la herramienta de gestión de incidencias, el correspondiente incidente de seguridad.
- Los usuarios deben utilizar contraseñas seguras de acuerdo a la política de contraseñas que MISTRAL establezca.
- Si, en un momento dado, un usuario recibiera una llamada telefónica solicitando su nombre de usuario y contraseña, nunca facilitará dichos datos y procederá a comunicar este hecho al Responsable de Seguridad, de forma inmediata.

10 USO DEL CORREO ELECTRÓNICO

El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios de Aula Abierta, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas.

Se trata de un recurso compartido por todos los usuarios de la organización, por lo que un uso indebido del mismo repercute de manera directa en el servicio ofrecido a todos.

Por ello, se dictan las siguientes normas de uso.

Normas generales

- Todos los usuarios que lo precisen para el desempeño de su actividad profesional dispondrán de una cuenta de correo electrónico, para el envío y recepción de mensajes internos y externos a la organización.
- Únicamente podrán utilizarse las herramientas y programas de correo electrónico suministrados, instalados y configurados por Aula Abierta.

- El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal, evitando el uso privado del mismo.
- Ningún mensaje de correo electrónico será considerado como privado en ninguno de sus componentes y especialmente en su parte correspondiente al encabezamiento.
- Se considerará correo electrónico tanto el interno, entre terminales de la red corporativa, como el externo, dirigido o proveniente de otras redes públicas o privadas, y, especialmente, Internet.
- Se deberá notificar al Responsable de Seguridad a través del correo cualquier tipo de anomalía detectada, así como un alto volumen de correos no deseados (spam) que se reciban, a fin de configurar adecuadamente las medidas de seguridad oportunas.
- Se deberá prestar especial atención a los ficheros adjuntos en los correos recibidos. No deben abrirse ni ejecutar ficheros de fuentes no fiables, puesto que podrían contener virus o código malicioso. En caso de duda sobre la confiabilidad de los mismos, se deberá notificar esta circunstancia al Responsable de Seguridad.
- Está terminantemente prohibido suplantar la identidad de un usuario de internet, correo electrónico o cualquier otra herramienta colaborativa.
- Cuando un usuario deje de tener relación con la institución, su cuenta será desactivada, lo que implica que la dirección de correo electrónico que tiene asignada es dada de baja y su buzón eliminado del servidor.

Usos especialmente prohibidos

Las siguientes actuaciones están explícita y especialmente prohibidas:

- El envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad, que contengan programas informáticos (software) sin licencia, que vulneren los derechos de propiedad intelectual de los mismos, de alerta de virus falsos o difusión de virus reales y código malicioso, o cualquier otro tipo de contenidos que puedan perjudicar a los usuarios, identidad e imagen corporativa y a los propios sistemas de información de la organización.
- El acceso a un buzón de correo electrónico distinto del propio y el envío de correos electrónicos con usuarios distintos del propio.

- La difusión de la cuenta de correo del usuario en listas de distribución, foros, servicios de noticias, etc., que no sean consecuencia de la actividad profesional del usuario.
- Responder mensajes de los que se tenga sospechas sobre su autenticidad, confiabilidad y contenido, o mensajes que contengan publicidad no deseada.
- La utilización del correo corporativo como medio de intercambio de ficheros especialmente voluminosos sin autorización, y el envío de información sensible, confidencial o protegida.

11 ACCESO A INTERNET Y HERRAMIENTAS DE TRABAJO

El acceso corporativo a Internet es un recurso centralizado que Aula Abierta pone a disposición de los usuarios, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional.

Aula Abierta velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso.

Normas generales

- El uso del sistema informático de Aula Abierta para acceder a redes públicas como Internet, se limitará a los temas directamente relacionados con la actividad de Aula Abierta y los cometidos del puesto de trabajo del usuario.
- Las conexiones que se realicen a Internet deben obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos. El acceso a Internet para fines personales debe limitarse y, de ser absolutamente necesario, sólo debe utilizarse un tiempo razonable, que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.
- Se prohíbe el uso de navegador alternativo, sin la debida autorización del Responsable de Seguridad.
- Deberá notificarse al Responsable de Seguridad de Aula Abierta cualquier anomalía detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

- Aula Abierta se reserva el derecho a monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa.
- Cualquier fichero introducido en la red corporativa de Aula Abierta o en el terminal del usuario desde Internet, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

Usos específicamente prohibidos

Quedan prohibidas las siguientes actuaciones:

- La descarga de programas informáticos o ficheros con contenido dañino que supongan una fuente de riesgos para la organización.
- El acceso a debates en tiempo real (Chat / IRC) es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido.
- El acceso a recursos y páginas-web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.
- La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.).

12 TRABAJO A DISTANCIA

El trabajo a distancia es una modalidad laboral que permite a los empleados realizar sus funciones fuera de las instalaciones de la empresa, utilizando tecnologías de la información y comunicación. **No se considera trabajo a distancia el uso ocasional de equipos portátiles fuera de la empresa.**

El trabajo a distancia deberá ser autorizado previamente por la **Dirección**, mediante comunicación directa con el empleado o los empleados afectados.

Durante el trabajo a distancia el empleado deberá tener en cuenta las siguientes medidas:

- Está prohibida la descarga de información de los equipos de la empresa sin autorización expresa.
- El usuario deberá conectarse exclusivamente a través de una VPN corporativa.
- La red Wi-Fi utilizada para el trabajo a distancia deberá:
    - Contar con una **contraseña segura**, conforme a la política de contraseñas de la empresa.
    - Ser de uso exclusivo para los dispositivos corporativos.
    - La red local utilizada para la conexión a Internet deberá estar configurada de forma segura para evitar vulnerabilidades.
- El trabajador a distancia debe evitar el acceso no autorizado por parte de cualquier persona ajena a la empresa, incluidas aquellas que compartan el mismo espacio físico de trabajo.
- Queda prohibido el uso de información confidencial en formato físico, así como el uso de impresoras personales para documentos de la empresa.
- Se deberá garantizar la protección de los derechos de propiedad intelectual de la organización, tanto en software como en cualquier otro contenido protegido.
- Todo material desarrollado durante la jornada de teletrabajo será propiedad de Aula Abierta.

  El empleado deberá asegurarse de que **niños, mascotas u otras personas** no tengan acceso a los dispositivos corporativos.

13 INCIDENTES DE SEGURIDAD

- Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de Aula Abierta o su imagen, deberá informar inmediatamente al Responsable de Seguridad, que lo registrará debidamente y elevará, en su caso a través de la aplicación de gestión de incidencias.
- Cuando las averías o incidencias comprometan la seguridad de datos de carácter personal, los usuarios harán uso del procedimiento de notificación de incidencias de carácter personal habilitado por el responsable de seguridad. El Responsable de

Seguridad dará el soporte necesario para su resolución y procederá a su anotación en el registro de incidencias.

- Dicha comunicación deberá realizarse inmediatamente y, en cualquier caso, en un plazo de tiempo no superior a una hora desde el momento en que se conozca dicha incidencia.

- El conocimiento y la no notificación de una incidencia por parte de un usuario serán considerados como una falta contra la seguridad de la información perteneciente a Aula Abierta, por su parte.

- El procedimiento sobre la gestión de incidentes se constata en el Procedimiento de gestión de incidentes.docx

14 COMPROMISO DE LOS USUARIOS

Es responsabilidad directa del usuario:

- Custodiar las credenciales que se le proporcionen para garantizar que aquellas no puedan ser utilizadaspor terceros. Deberá cerrar su cuenta al terminar la sesión o bloquear el equipo cuandolo deje desatendido.

- En el caso de que su equipo contenga información sensible, confidencial o protegida, esta deberá cumplir todos los requisitos legales aplicables y las medidas de protección que la normativa de Aula Abierta establezca al respecto.

- Además de lo anterior, no se podrá acceder a los recursos informáticos y telemáticos de Aula Abierta para desarrollar actividades que persigan o tengan como consecuencia:

  - El uso intensivo de recursos de proceso, memoria, almacenamiento ocomunicaciones, para usos no profesionales.
  - La degradación de los servicios.
  - La destrucción o modificación no autorizada de la información, de manera premeditada.
  - La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.

- El deterioro intencionado del trabajo de otras personas.
- El uso de los sistemas de información para fines ajenos a los de Aula Abierta, salvo aquellas excepciones que contempla la presente Normativa.
- Dañar intencionadamente los recursos informáticos de Aula Abierta o de otras instituciones.
- Incurrir en cualquier otra actividad ilícita, del tipo que sea.

15 MONITORIZACIÓN Y APLICACIÓN DE LA NORMATIVA

Aula Abierta, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

- Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
- Monitorizará los accesos a la información contenida en sus sistemas.
- Auditará la seguridad de las credenciales y aplicaciones.
- Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.

MISTRAL llevará a cabo esta actividad de monitorización sin utilizar sistemas o programas que pudieran atentar contra los derechos constitucionales de los usuarios, tales como el derecho a la intimidad personal y al secreto de las comunicaciones, manteniéndose en todo momento la privacidad de la información manejada, salvo que, por requerimiento legal e investigación sobre un uso ilegítimo o ilegal, sea necesario el acceso a dicha información, salvaguardando en todo momento los derechos fundamentales de los usuarios.

Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca. El Responsable de Seguridad, con la colaboración de las restantes unidades de Aula Abierta, velará por el cumplimiento de la presente Normativa General e informará al Comité de Seguridad sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente

Normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar.

16 PUESTO DESPEJADO Y PANTALLA LIMPIA

Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos etiquetados como confidenciales, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos.

No se debe consumir alimentos ni bebidas cerca de los equipos, ya que los derrames generalmente ocasionan cortocircuitos en los mismos con el consiguiente riesgo de daño del equipo y pérdida de información.

Este tipo de documentos y soportes deben ser archivados de forma segura, de acuerdo con lo establecido en la ***Política de Clasificación de la Información.***

16.1 Política de pantalla limpia

Los puestos de trabajo deben, preferentemente, ubicarse en lugares que no queden expuestos al fácil acceso de cualquier persona.

Los equipos que queden ubicados cerca de las zonas de atención o tránsito público deben situarse de forma que las pantallas de trabajo no queden expuestas y puedan ser visualizadas por personas no autorizadas.

Si la persona autorizada no se encuentra en su puesto de trabajo, se debe quitar toda la información sensible de la pantalla y se debe denegar el acceso a todos los sistemas para los cuales la persona tiene autorización.

En el caso de una ausencia corta (hasta 15 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas o bloqueando la pantalla con una clave.

16.2 Protección de instalaciones y equipos compartidos

Los documentos que contienen información sensible deben ser retirados inmediatamente de las impresoras, equipos de fax y fotocopiadoras.

Se evitará que personal no autorizado pueda acceder a impresoras, fotocopiadoras, escáneres y demás equipamiento compartido para copiado.

Los equipos de reproducción de información como: impresoras, fotocopiadoras, escáneres o similares, deben estar, en la medida de lo posible, en lugares ubicados con acceso controlado, y cualquier documentación, sobre todo confidencial, debe ser recuperada de manera inmediata por el responsable de su generación.

Al finalizar la jornada laboral, los empleados deben guardar en lugar seguro los documentos y medios que contengan información confidencial o de uso interno. Además, deberán cerrar las aplicaciones o servicios que hayan utilizado y apagar su equipo.

16.3 Salas y pizarras limpias.

Las salas o áreas de reuniones deben quedar limpias de todo el material utilizado.

Después de las reuniones en las que se utilicen pizarras, éstas deben quedar limpias de información que se ha expuesto en ellas, sobre todo si su tratamiento debiera ser uso interno o confidencial.

En caso de que se utilice un equipo de trabajo para presentaciones, debe eliminarse la información antes prestada, sobre todo si su tratamiento debiera ser de uso interno o confidencial.

Al finalizar eventos, que precisen de equipos de proyección, audio o similar, quienes hayan hecho uso de estos deben asegurarse de apagarlos por completo.

17 PROCESO DISCIPLINARIO

Todos los usuarios de Aula Abierta están obligados a cumplir lo prescrito en la presente Normativa de Seguridad de la Información.

Los trabajadores serán conscientes que el convenio de los trabajadores de aplicación establece como falta muy grave*: Violación de los secretos de obligada confidencialidad, el*

de correspondencia o documentos reservados de la empresa, debidamente advertida, revelándolo a personas u organizaciones ajenas a la misma, cuando se pudiera causar perjuicios graves a la empresa.

En caso de que un usuario realice una violación de la seguridad o generado una brecha de seguridad, Dirección y/o RSGI abrirán una investigación para determinar de forma imparcial su responsabilidad y valorar una posible intencionalidad o negligencia. La empresa, siempre desde la imparcialidad y legalidad, tomará acciones disciplinarias contra el empleado en función de la gravedad, intencionalidad y daños generados. En los casos más graves se podría llegar a despedir al empleado y exigirle responsabilidades penales.

Al término de la relación laboral con el empleado, éste deberá seguir manteniendo la confidencialidad suscrita con la firma de su contrato. Dirección recordará estos términos. El usuario devolverá todos sus dispositivos, activos y cualquier otro medio del que disponga acceso a la información de la empresa. El Responsable de Seguridad de la Información procederá al cambio de contraseñas y cualquier otro tipo de clave de acceso a la información de los sistemas.

El procedimiento a seguir para iniciar un **proceso disciplinario** cuando un trabajador ponga en riesgo la seguridad de la información de forma intencionada o por negligencia, será el siguiente:

- Investigación: Se llevará a cabo una investigación completa y justa sobre el presunto incumplimiento de las políticas de seguridad de la información. Esto puede implicar la recopilación de pruebas, entrevistas con testigos y revisión de registros relevantes.
- Entrevista con el empleado: El empleado será convocado a una reunión con su supervisor o el departamento de recursos humanos para discutir las acusaciones en su contra. Durante esta entrevista, se proporcionará al empleado la oportunidad de explicar su versión de los hechos.
- Determinación de la culpabilidad: Basado en la investigación y la entrevista con el empleado, se determinará si el empleado ha violado las políticas de seguridad de la información de la empresa.
- Advertencia: En caso de que se confirme el incumplimiento, se emitirá una advertencia al empleado por escrito. Esta advertencia incluirá detalles sobre el incidente, las políticas violadas y las posibles consecuencias adicionales en caso de futuros incumplimientos.
- Seguimiento: Se establecerá un plan de seguimiento para monitorear el cumplimiento continuo del empleado con las políticas de seguridad de la información. Esto puede incluir capacitación adicional, supervisión adicional o cualquier otra medida correctiva necesaria.

- Registro: Se mantendrá un registro detallado de todas las etapas del proceso disciplinario, incluida la investigación, la entrevista con el empleado, la determinación de la culpabilidad y las acciones tomadas.

El empleado tendrá el derecho de apelar la advertencia emitida dentro de un período de tiempo especificado, proporcionando evidencia adicional o argumentando contra las conclusiones del proceso disciplinario.

Este protocolo será revisado periódicamente para garantizar su efectividad y su alineación con las políticas de seguridad de la información de la empresa. Cualquier revisión o actualización será comunicada a todos los empleados de manera oportuna.

18 HISTÓRICO DE CAMBIOS

EDICIÓN	MOTIVO DEL CAMBIO	FECHA DE APROBACIÓN	APROBADO POR
1.0	Elaboración y aprobación	20/03/2026	Responsable de Seguridad