Procedimiento de Gestión de Usuarios. (Uso Interno)

Ediciones y Revisiones

Fecha	Edición	Descripción del cambio
28/06/2021	00	Edición inicial

Elaboración y Aprobación

Elaborado por: Resp. de sistema gestión **Fecha: 28/06/2021**	**Aprobado por: Gerencia** **Fecha: 28/06/2021**

1. Objetivo

El Objeto del presente documento es definir el Procedimiento aplicable a la Gestión de RRHH en las incorporaciones y las bajas del personal de ESCLAPÉS E HIJOS S.L.
Así como, establecer el procedimiento a seguir para establecer contraseñas acordes a los requisitos legales vigentes que debe ser aplicada a cualquier mecanismo de autenticación que utilicen los miembros de ESCLAPÉS E HIJOS S.L.

2. Alcance

Este procedimiento será de aplicación a todas las nuevas incorporaciones y las bajas de personal de ESCLAPÉS E HIJOS S.L, así como a el personal que de manera permanente o eventual esté vinculado a ESCLAPÉS E HIJOS S.L.

3. Actualización del documento

Cuando se produzca un cambio significativo en la estructura o en la operativa de ESCLAPÉS E HIJOS S.L que afecte a este procedimiento, deberá producirse una modificación y actualización del mismo.
Se notificará al Comité de Seguridad de los cambios y modificaciones identificados, y éstos serán incluidos en una nueva versión del documento, así como en el apartado de control de cambios, como evidencia del proceso de actualización realizado y para mantener la trazabilidad entre distintas versiones.
Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

4. Detalle de Proceso de incorporación de trabajadores

4.1. Incorporación de Trabajadores

Previamente a la contratación, indefinida o temporal, de un empleado en ESCLAPÉS E HIJOS S.L , el Gerente de la empresa realiza las siguientes comprobaciones acerca de su currículum o perfil:

- Confirmación de identidad y nacionalidad, mediante DNI o equivalente. En el caso de trabajadores extranjeros, debe solicitarse un visado válido.
- Solicitud de títulos académicos y profesionales, si así se requiere en el puesto de trabajo.

ESCLAPÉS E HIJOS S.L dispone de fichas de “Descripciones de funciones y responsabilidades” en las que claramente se han definido las competencias necesarias para desarrollar trabajos para los que han sido contratados. En las mismas se determinan el diseño curricular y la experiencia necesaria que se necesita para cubrir dicho puesto de trabajo.

Antes de la incorporación de cualquier empleado, el Responsable de Administración comprueba que cumple los requisitos mínimos que se han definido en las “Descripciones de funciones y responsabilidades”. Si no los cumpliera, se debería planificar la formación necesaria para que los obtenga con la mayor brevedad posible.

Dirección se encarga de:

- Preparar y entregar el **Acuerdo de Confidencialidad** y la comunicación informativa del tratamiento de datos personales al nuevo empleado, requiriéndole su devolución una vez firmado.
- Gestionar el alta laboral del nuevo empleado con el asesor y asignarle los activos.

- Entregar Manual de Políticas, Normas de Uso y Seguridad de la Información y demás procedimientos que le apliquen según su puesto de trabajo.
- Entrega de información de Prevención de Riesgos Laborales
- Alta en el sistema
- Asignación de PC. El usuario debe de hacerse responsable del mismo y comprometerse a reportar cualquier incidente y entregarlo en perfecto estado.
- Asignación de privilegios de usuario. Los propietarios de la información deben definir los niveles de acceso de cada usuario.
- Asignación de email, teléfono, permisos en servidor de archivos.
- Configuración acceso a zonas restringidas.
- A los nuevos empleados, se les indica la ubicación de la documentación, tanto procedimientos como registros para que conozcan las políticas y metodologías de trabajo a seguir.

La empresa se compromete a tener permanentemente actualizados los conocimientos de seguridad de todos sus empleados, comunicándoles de manera inmediata cualquier hecho o novedad relevante que se produzca, y procurando atender a su formación permanente en esta materia, recurriendo siempre que ello sea posible a la asistencia a cursos externos de formación sobre temas o asuntos de seguridad a los que se pudiera tener acceso.

Deben existir mecanismos de información y capacitación para los usuarios en materia de seguridad, así como de reporte de incidentes que puedan afectarla. Los empleados deben cooperar con los esfuerzos por proteger la información y ser responsables de actualizarse en cada materia, así como consultar con el responsable de la seguridad de la información, en caso de duda o desconocimiento de un procedimiento formal, ya que esto no lo exonera de una acción disciplinaria que deba llevarse a cabo cuando se incurra en violaciones a las políticas o normas de seguridad.

4.2.Bajas de Trabajadores

Cuando cesa la actividad de un empleado en la plantilla de ESCLAPÉS E HIJOS S.L, se realizan las siguientes acciones:

- Revocación total de los derechos de acceso corporativos (correo electrónico, acceso remoto (si lo hubiese), etc…)
- Gestionar la baja laboral con asesor
- Recordar al empleado su compromiso de confidencialidad
- Supresión de credenciales lógicas.
- Retirada de activos físicos (móviles, equipos u otros).
- Retirada de activos de acceso, tarjetas, llaves y otros que pudieran haberse asignado.
- Deshabilitado de cuentas.
- Deshabilitado de acceso físico.
- Notificación al resto del equipo / compañeros del cambio y en caso de que corresponda, recordar los compromisos de confidencialidad con suministrar información a personal externo a la organización, recordando que este último ya no pertenece a la misma.
- Durante el periodo de mes y medio se mantendrá activa la cuenta de correo desviada al Responsable de Seguridad. Pasado éste periodo se dará de baja. Nunca se enviarán correos electrónicos desde un correo electrónico de otro trabajador,

Si es necesario un abandono inminente de las instalaciones, un responsable de departamento o en su defecto el Gerente debe acompañar al empleado hasta el exterior de las oficinas de ESCLAPÉS E HIJOS S.L.

4.3.Altas Personal Externo

Cuando exista la necesidad de otorgar acceso a terceras partes a información de la empresa, el Responsable del Sistema y el propietario de la información de que se trate llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso)
- Los motivos para los cuales se solicitan el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte
- La incidencia de este acceso en la seguridad de la información de la Organización.

La Dirección se encarga de:

- Preparar y entregar el **Acuerdo de Confidencialidad**
- Entregar Manual de Políticas, Normas de Uso y Seguridad de la Información y demás procedimientos que le apliquen según su puesto de trabajo.

Dirección enviará un correo electrónico al Responsable del Sistema, indicándole las necesidades del nuevo usuario incluyendo la siguiente información:

- Nombre y Apellidos
- Trabajos que va a ejecutar
- Empresa
- Fecha de incorporación
- Fecha prevista de finalización

4.4.Bajas personal Externo

El Responsable de Sistemas realizará un seguimiento de las fechas de expiración de las credenciales de identificación del personal externo. Dirección confirmará si es necesario la renovación o no de las credenciales, en caso de que lo sea comunicará al Responsable del Sistema una nueva fecha prevista de finalización.

Una vez finalizados los trabajos contratados, el Responsable del Sistema:

- Ejecutará las acciones pertinentes para dar de baja al usuario externo de los sistemas, en la fecha señalada.
- En el caso de que tuviera asignado un equipo, retirará tal equipo.
- Reclamará al personal externo la devolución del material informático facilitado por la Organización.

4.5.Gestión de privilegios

Los privilegios de acceso de los usuarios a los Sistemas de Información deben ser gestionados y controlados adecuadamente para evitar accesos o usos no autorizados de la información y de los sistemas que la soportan. Para ello se realizarán revisiones periódicas de los privilegios asignados, que posibiliten la adopción de las medidas correctivas, en su caso.

- Solo se permitirá el acceso a los recursos cuando exista una necesidad legítima para el desarrollo de las actividades profesionales del usuario. Por otro lado, los permisos otorgados a cada usuario deberán ser los mínimos para el desarrollo de sus funciones.
- Se mantendrá un Inventario para el Control de Accesos, en el que se identifiquen los usuarios y los privilegios autorizados y denegados.
- Los soportes y documentos que contengan datos de carácter personal serán accesibles únicamente por el personal autorizado.
- La información se creará al dar de alta a un usuario por primera vez en alguno de los sistemas afectados, y deberá mantenerse actualizada, registrándose todas aquellas

modificaciones que se produzcan en los privilegios de acceso hasta el momento en el que el usuario haya causado baja en todos los sistemas.

- Al menos una vez al año se realizará una revisión de los privilegios de acceso de todos los usuarios.
- Cuando se trate de privilegios especiales (administrador, root, etc..) tal revisión debe realizarse siempre que se produzca un alta de nuevos usuarios ó baja de usuarios.
- Todos los privilegios de accesos de usuarios tanto internos como externos deben ser cancelados en el momento de la finalización de su contrato o prestación de servicios en la Organización.

5. Desarrollo del control de acceso lógico de los usuarios

A todo usuario de **ESCLAPÉS E HIJOS S.L**, tanto propio como ajeno, se le asignará un usuario dependiendo del nivel de acceso necesario para la ejecución de sus funciones. El cual deberá cumplir con los procedimientos establecidos, aplicar las normas y procedimientos operativos de seguridad de **ESCLAPÉS E HIJOS S.L**.

5.1. Política de contraseñas

Parámetro	Valor
Caducidad de contraseñas	6 meses, excepto para contraseñas de administración de sistemas
Reutilización de contraseñas	Ninguna de las 3 últimas
Longitud	Mínimo 8 caracteres
Características de la contraseña	• La contraseña debe contener al menos 4 caracteres alfabéticos de los cuales serán, al menos, dos letras mayúsculas y dos minúsculas. • La contraseña debe contener al menos 2 caracteres numéricos. • El número máximo de repeticiones de caracteres adyacentes de la contraseña será 4. • El número máximo de caracteres numéricos en secuencia de la contraseña será 4. • La contraseña no podrá contener el nombre o apellido del usuario, ni el documento de identidad del mismo. • No se podrán utilizar las tres últimas contraseñas empleadas. • Modificar la contraseña que le entreguen antes de hacer uso de ella aunque no esté obligado a hacerlo. • Tener al menos un símbolo (cualquier otro carácter que no sea alfabético o numérico: ` ~! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /).
Suspensión de autenticadores	Tras 3 meses sin su utilización.
Intentos fallidos	Tras 5 intentos se bloquea a cuenta de usuario
Limitación de horarios, fechas y lugar de acceso	Si o si desde nivel medio debe de haber una limitación.
Cautelas generales	Las contraseñas iniciales deben ser generadas automáticamente y se cambiaran en el primer acceso a los sistemas El número de intentos de acceso sin éxito consecutivos debe estar limitado. Los salvapantallas deben tener activada la protección por contraseña, bloqueándose tras un periodo de inactividad. Deben de existir mecanismos de expiración y caducidad de contraseña para obligar a los usuarios al cambio de la misma.

5.2. ALMACÉN DE CONTRASEÑAS

Las claves se almacenan cifradas en el fichero ……

5.3.REVISIÓN DE USUARIOS Y ACCESOS NO AUTORIZADOS

El personal tanto propio como ajeno, relacionado con los sistemas de información sujetos a la seguridad de la información de **ESCLAPÉS E HIJOS S.L**, será formado e informado de sus deberes y obligaciones en materia de seguridad. Su actuación, será supervisada para verificar que se siguen los procedimientos establecidos, que se aplican las normas y los procedimientos operativos de seguridad en el desempeño de sus tareas.

Al menos, cada <<señalar periodicidad>>, se realizará una revisión de los privilegios de acceso de todos los usuarios y de los derechos de acceso asignados. Los derechos de acceso privilegiados deberán revisarse con una periodicidad menor. Esta periodicidad será de <<señalar periodicidad>.

Cuando se trate de privilegios especiales (administrador, root, etc.), tal revisión de privilegios se deberá realizar, al menos, cada <<señalar periodicidad>>, y, en cualquier caso, siempre que existan:

- Alta de nuevos usuarios
- Baja de usuarios

Además de lo anterior, deberá realizarse una revisión de los permisos de acceso correspondientes a los usuarios, tanto internos como externos, siempre que hubiere sufrido modificación significativa de sus funciones ó responsabilidades.

Para ambos tipos de usuarios se tendrán en cuenta, al menos, las siguientes cuestiones:

- Necesidad de nuevos permisos.
- Cancelación de antiguos permisos.
- Segregación de funciones.
- Devolución de activos y modificación o cancelación de permisos de accesos físicos.
- Modificación de contraseñas de acceso.
- Notificación al personal implicado de su baja o cambio.
- Necesidad de retención de registros.

Siempre que se dé de baja un usuario, su usuario quedará bloqueado durante 3 meses, transcurrido dicho plazo, el usuario será eliminado del sistema.

5.4.MODIFICACION DE LOS PRIVILEGIOS DE ACCESO

La asignación, modificación o revocación de privilegios en los Sistemas de Información del ESCLAPÉS E HIJOS S.L será solicitada por los responsables del departamento o área a la que pertenezca el destinatario de dichos privilegios.

La modificación de privilegios vendrá precedida de una solicitud por escrito del responsable del departamento al que va a concedérsele acceso y deberá mantenerse actualizada, registrándose todas aquellas modificaciones que se produzcan en los privilegios de acceso hasta el momento en que el usuario haya causado baja en todos los sistemas incluidos en el alcance.

5.5.MECANISMOS DE AUTENTICACIÓN

Sistema/Servicio	Mecanismo
RP	Usuario y contraseña
Correo electrónico	Usuario y contraseña

5.6. MONITORIZACIÓN DE LOS ACCESOS

La organización realiza labores periódicas de monitorización de los sistemas con el fin de detectar accesos no autorizados y desviaciones, registrando eventos que suministren evidencias en caso de producirse incidentes relativos a la seguridad.
A tal efecto, se tendrán en cuenta:

- Registro de eventos: intentos de acceso fallidos, bloqueo de cuenta, debilidad de contraseñas, normalización de identificadores, cuentas inactivas….
- Registro de uso de sistemas: accesos no autorizados, uso de privilegios, alertas de sistema.

Todos los equipos que cuentan con un reloj interno están sincronizados entre sí para garantizar a precisión de los sucesos registrados y permitir la correlación de los diferentes eventos.

6. ARCHIVO Y REGISTROS

Código	Descripción	Responsable	Periodo
	Curriculum	Resp. Sistema	3años
	Acuerdo de confidencialidad	Resp. Sistema	3años
	Manual de políticas, normas de uso y seguridad de la información	Resp. Sistema	3 años