DATOS

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																										
	Clasificación				Actos originados por la criminalidad común y motivació								Sucesos de origen físico						Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales												
Datos e Información	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen)	Impacto de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sabotaje (ataque físico y electrónico)	Actos mal intencionados	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión / infiltración a Red interna	Virus / Ejecución no autorizado de programas	Ingeniería Social	Incendio	Inundación	Sismo	Falta de mantenimiento preventivo y correctivo	Falla de energía	Falla de sistema / HW,SW o Comunicaciones	Mal manejo de sistemas y herramientas	Comunicación inadecuada	Pérdida de datos	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	No divulgación de información institucional	Uso inadecuado de la imagen institucional	Baja presencia en los medios de comunicación externos	Compartir contraseñas o permisos a terceros	Descontrol de la información publicada en redes sociales	Falta de definición de perfil, privilegios y restricciones del personal	Colapso de los sistemas de información	Falta de actualización de software (proceso y recursos)	Violación del sistema. Acceso electrónico no autorizado	Ausencia de documentación
					1	1	1	1	1	3	1	2	1	1	2	1	2	1	2	2	1	2	2	1	2	1	2	1	1	1	2	1
Documentos institucionales	x	x	x	2	2	2	2	2	2	6	2	4	2	2	4	2	4	2	6	9	2	9	4	9	4	2	9	2	9	6	4	2
Directorio de Contactos	x			1	1	1	1	1	1	3	1	2	1	1	2	1	2	1	2	2	1	2	2	1	2	2	4	1	6	1	2	1
Productos institucionales (Folletos, Fotos, etc.)			x	1	1	1	1	1	1	9	1	2	1	1	2	1	2	9	9	9	6	9	6	9	9	6	2	6	9	1	4	1
Informática (Planes, Documentación, etc.)		x		1	1	1	1	1	1	3	1	2	1	1	2	1	2	1	2	8	8	12	12	8	8	6	2	6	8	1	4	2
Serv. Consulta Generales (Comparendos, Estado de Tramites)		x	x	2	2	2	2	2	2	12	2	4	2	2	4	2	4	12	8	8	8	12	6	8	12	8	8	8	8	4	6	2
Serv. Manejo PQRS		x	x	2	2	2	2	2	2	8	2	4	2	2	4	2	4	8	8	8	8	12	8	8	8	8	8	6	8	4	4	2
Serv. Chat Online			x	1	1	1	1	1	1	4	1	2	1	1	2	1	2	4	4	8	4	6	6	6	2	12	4	12	8	4	4	1
Serv. Tramites en Linea	x	x	x	3	3	3	3	3	3	12	3	6	3	3	6	3	6	12	8	8	8	8	8	8	6	8	8	8	8	4	4	3
Página Web interna (Intranet)	x		x	2	2	2	2	2	2	9	2	4	2	2	4	2	4	9	9	9	9	9	9	9	4	9	4	9	9	4	4	2
Sitio Web		x	x	3	3	3	3	3	3	12	3	6	3	3	6	3	6	12	8	8	12	12	8	8	6	6	12	8	8	4	6	3

SISTEMA

Matriz de Análisis de Riesgo					1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																					
	Clasificación				inalidad común y motivación				Sucesos de origen físico						Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales												
Sistemas e Infraestructura	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen)	Impacto de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Robo / Hurto de información electrónica	Intrusión / infiltración a Red interna	Virus / Ejecución no autorizado de programas	Ingeniería Social	Incendio	Inundación	Sismo	Falta de mantenimiento preventivo y correctivo	Falla de energía	Falla de sistema / HW,SW o Comunicaciones	Mal manejo de sistemas y herramientas	Comunicación inadecuada	Pérdida de datos	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	No divulgación de información institucional	Uso Inadecuado de la imagen institucional	Baja presencia en los medios de comunicación externos	Compartir contraseñas o permisos a terceros	Descontrol de la información publicada en redes sociales	Falta de definición de perfil, privilegios y restricciones del personal	Colapso de los sistemas de información	Falta de actualización de software (proceso y recursos)	Violación del sistema. Acceso electrónico no autorizado	Ausencia de documentación
					1	3	1	2	1	1	2	1	2	1	2	2	1	2	2	1	2	1	2	1	1	1	2	1
Equipos de la red cableada (router, switch, etc.)	x		x	3	3	9	3	6	3	3	6	3	6	3	6	6	3	6	6	3	6	3	6	3	3	3	6	3
Equipos de la red inalámbrica (router, punto de acceso, etc.)	x		x	3	3	9	3	6	3	3	6	3	6	3	6	6	3	6	6	3	6	3	6	3	3	3	6	3
Firewall	x		x	4	4	9	4	8	4	4	8	4	8	4	8	8	4	8	8	4	8	4	8	4	4	4	8	4
Servidores	x		x	4	4	9	4	8	4	4	8	4	8	4	8	8	4	8	8	4	8	4	8	4	4	4	8	4
Aplicaciones (Software)	x		x	4	4	9	4	8	4	4	8	4	8	4	8	8	4	8	8	4	8	4	8	4	4	4	8	4
Bases de Datos		x	x	4	4	9	4	8	4	4	8	4	8	4	8	8	4	8	8	4	8	4	8	4	4	4	8	4
Equipos de Cómputo	x	x	x	2	2	6	2	4	2	2	4	2	4	2	4	4	2	4	4	2	4	2	4	2	2	2	4	2
Respaldo Datos	x		x	4	4	9	4	8	4	4	8	4	8	4	8	8	4	8	8	4	8	4	8	4	4	4	8	4
Programas de comunicación (correo electrónico, chat, llamadas telefónicas PBX,	x	x	x	2	2	6	2	4	2	2	4	2	4	2	4	4	2	4	4	2	4	2	4	2	2	2	4	2
Scanner	x		x	1	1	3	1	2	1	1	2	1	2	1	2	2	1	2	2	1	2	1	2	1	1	1	2	1
Infraestructura física	x		x	4	4	9	4	8	4	4	8	4	8	4	8	8	4	8	8	4	8	4	8	4	4	4	8	4

PERSONAL

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																												
Personal	Clasificación			Impacto de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común y motivació								Sucesos de origen físico						Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales													
	Imagen pública de alto perfil, indispensable para funcionamiento institucional	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional		Sabotaje (ataque físico y electrónico)	Actos mal intencionados	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión / infiltración a Red interna	Virus / Ejecución no autorizado de programas	Ingeniería Social	Incendio	Inundación	Sismo	Falta de mantenimiento preventivo y correctivo	Falla de energía	Falla de sistema / HW, SW o Comunicaciones	Mal manejo de sistemas y herramientas	Comunicación inadecuada	Pérdida de datos	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	No divulgación de información institucional	Uso Inadecuado de la imagen institucional	Baja presencia en los medios de comunicación externos	Compartir contraseñas o permisos a terceros	Descontrol de la información publicada en redes sociales	Falta de definición de perfil, privilegios y restricciones del personal	Colapso de los sistemas de información	Falta de actualización de software (proceso y recursos)	Violación del sistema. Acceso electrónico no autorizado	Ausencia de documentación
					1	1	1	1	1	3	1	2	1	1	2	1	2	1	2	2	1	2	2	1	2	1	2	1	1	1	2	1
Junta Directiva	x			2	2	2	2	2	2	6	2	4	2	2	4	2	4	2	4	8	2	4	12	8	12	2	6	2	2	2	2	6
Gerencia	x			3	3	3	3	3	3	8	3	6	3	3	6	3	6	3	6	8	3	4	12	8	12	3	6	3	3	8	2	3
Asesores		x		2	2	2	2	2	2	6	2	4	2	2	4	2	4	2	4	6	2	4	9	6	9	2	6	2	2	6	2	6
Profesional		x		3	3	3	3	3	3	9	3	6	3	3	6	3	6	3	6	6	3	9	6	6	6	6	6	3	6	6	6	6
Soporte Tecnico			x	1	1	1	1	1	1	3	1	2	1	1	2	1	2	1	2	2	9	9	2	1	2	6	2	1	6	6	6	1
Servicio de mensajería de externo			x	1	1	1	1	1	1	3	1	2	1	1	2	1	2	1	2	2	6	2	2	1	2	1	2	1	1	1	2	1

ANALISIS PROMEDIO

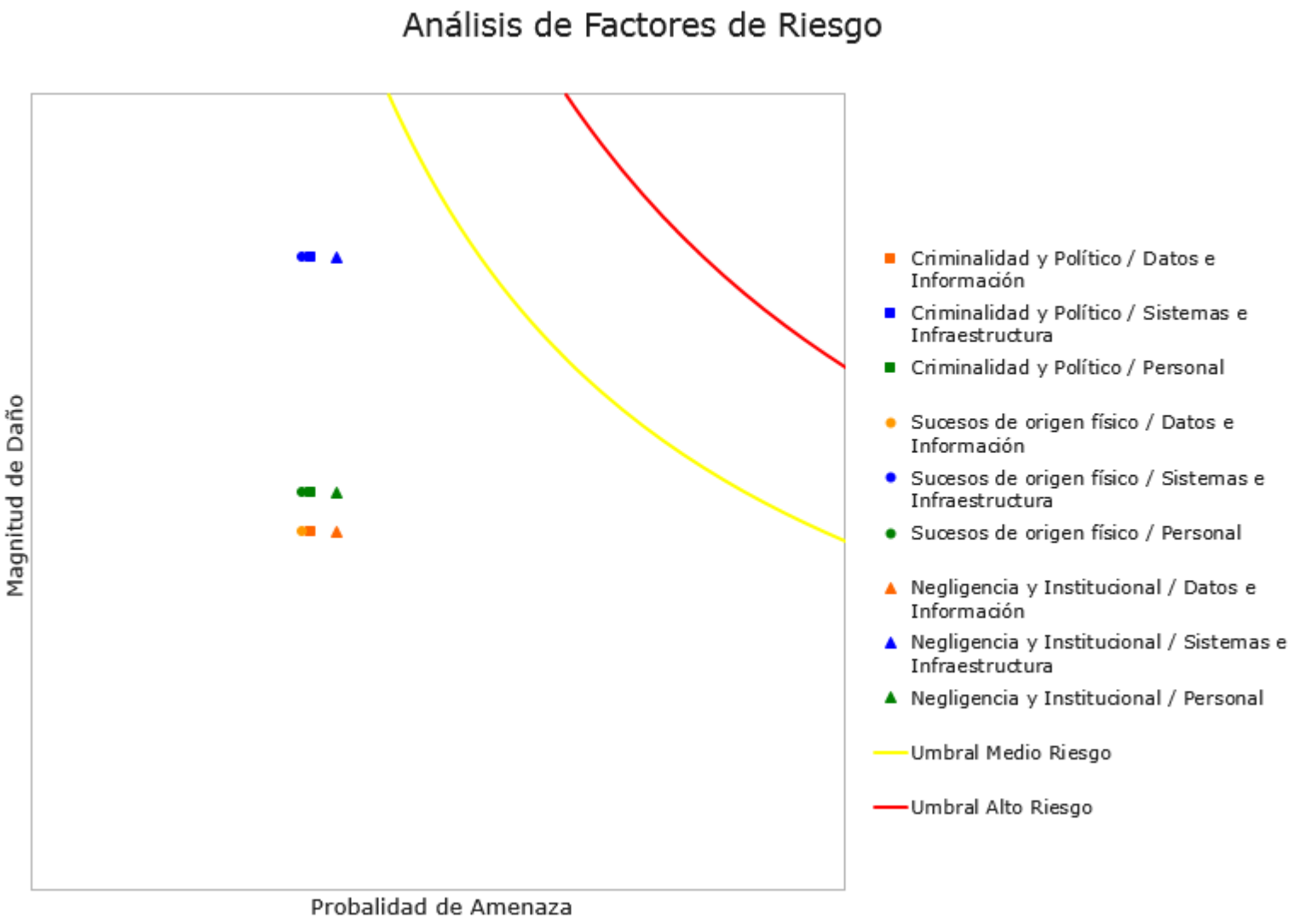
Análisis de Riesgo promedio

		Probabilidad de Amenaza		
		Criminalidad y Político	Sucesos de origen físico	Negligencia y Institucional
Magnitud de Daño	Datos e Información	2,8	3,3	6,2
	Sistemas e Infraestructura	4,2	4,2	4,8
	Personal	2,7	2,7	4,6

ANALISIS FINAL

Activo	Sub-Activo	Calificacion	Analisis
Esenciales	Serv. Consulta Generales (Comparendos, Estado de Tramites).	12	La no disonibilidad del sitio web traumatiza la operatividad del servicio, dado que el módulo de consultas, es la base fundamental que permite a los usuarios verificar los estados de sus trámites(comprendos,certificados de tradición)
Esenciales	Serv. Tramites en Linea	12	Los resultados arrojados por la matriz evidencian un riesgo muy alto que debe ser atendido, pues se muestra debilidad en la posibilidad de intrusión o infiltración al sistema de información que genera los trámites en línea y la administración del sitio Web.
Esenciales	Sitio Web	12	* Fallas en los sistemas de detección de intrusos afectan la integridad de la información contenidad en el sito web * Falta de compatibilidad entre las aplicaciones y el gestor de contenidos (joomla) por ser software libre. * Publicación irresponsable (sin autorización de la dirección) de artículos que afectan la imágen institucional.
Esenciales	Informática (Planes, Documentación, etc.)	12	El no cumplimiento de las leyes 1712(transparencia), 1474 (anticorrupción) establecen como de obligatorio cumplimiento la publicación de planes, resoluciones, procesos contractuales)acarreará sanciones.
Esenciales	Serv. Manejo PQRS	12	Las entidades del estado estan constantemente monitoreados por los entes de control que exigen medios de comunicación entre los usuarios y la entidad a fin de medir transparencia, así mismo lo exige gobierno en línea.
Esenciales	Serv. Chat Online	12	El decreto 019 del 2,012 (antitrámites) establece lineamientos destinados a la orientación y disminución de trámites a los usuarios del estado.
Personal	Junta Directiva	12	Violación de las políticas de seguridad al realizar solicitudes de operación sin el conocimiento necesario.
Personal	Gerencia	12	Violación de las políticas de seguridad al realizar solicitudes de operación sin el conocimiento necesario.

ANALISIS FACTORES



CONTROLES

Calificacion	Literal / Nombre	Descripción del Control	Responsable
12	10. Gestion de Comunicación y Operaciones 10.9 Servicio de Comercio Electrónico 10.9.3 Información Públicamente disponible	Se debería proteger la integridad de la información que pone a disposición en un sistema de acceso público para prevenir modificaciones no autorizadas	Jefe de Sistemas
12	10. Gestion de Comunicación y Operaciones 10.9 Servicio de Comercio Electrónico 10.9.2 Transacciones en línea	Se debería proteger la información involucrada en el comercio electrónico que pasa por redes publicas contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizadas.	Jefe de Sistemas
12	10. Gestion de Comunicación y Operaciones 10.9 Servicio de Comercio Electrónico 10.9.3 Información Públicamente disponible	Se debería proteger la integridad de la información que pone a disposición en un sistema de acceso público para prevenir modificaciones no autorizadas	Jefe de Sistemas
12	07. Gestión de Activos 7 2 Clasificación de la Información 7.2.1 Directrices de Clasificación	La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.	Jefe de Sistemas
	15.Cumplimiento 15.1 Conformidad con los requisitos legales 15.1.3. Salvaguarda de los registros de la Organización	Los registros importantes se deberían proteger de la pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios, regulaciones, contractuales y de negocio	Jefe de Sistemas
12	10. Gestión de Comunicaciones y Operaciones 10.10 Supervisión 10.10.1. Resgistros de auditoria	Se deberían producir y mantener durante un periodo establecido los registros de auditoria con la grabación de las actividades de los usuarios, excepciones y eventos de la seguridad de información, con el fin de facilitar las investigaciones futuras y el monitoreo de los controles de acceso.	Jefe de Sistemas
12	10. Gestión de Comunicaciones y Operaciones 10.8 Intercambio de información 10. 8. 4. Mensajería electrónica	Se debería proteger adecudamente la información contenida en la mensajería electrónica.	Jefe de Sistemas
12	08. Seguridad ligada a los Recursos Humanos 8 2 Seguridad en el desempeño de las funciones del empleo 8.2.2. Formación y capacitación en seguridad de la información	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo	Jefe de Sistemas
	08. Seguridad ligada a los Recursos Humanos 8 1 Seguridad en la definición del trabajo y los recursos 8.1.1. Inclusión de la seguridad en las	Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información	Jefe de Sistemas

12	06. Organización de la Seguridad de Información 6 1 Organización Interna 6.1.3. Asignación de responsabilidades	Se deberían definir claramente todas las responsabilidades para la seguridad de la información.	Jefe de Sistemas
9	07. Gestión de Activos 7.1 Responsabilidad sobre los activos 7.1. 3 Acuerdos sobre el uso adecuado	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos	Jefe de Sistemas
9	10. Gestión de Comunicaciones y Operaciones 10 1 Procedimientos y responsabilidades de operación 10.1.2. Control de cambios operacionales	Se deberían controlar los cambios en los sistemas y en los recursos de tratamiento de la información.	Jefe de Sistemas
	11. Control de Accesos 11. 2 Gestión de acceso de usuario 11.2.2. Gestión de privilegios	Se debería restringir y controlar la asignación y uso de los privilegios.	Jefe de Sistemas
	12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información 12 5 Seguridad en los procesos de desarrollo y soporte 12.5.1. Procedimientos de control de cambios	Se debería controlar la implantación de cambios mediante la aplicación de procedimientos formales de control de cambios.	Jefe de Sistemas
9	11. Control de Accesos 11.4 Control de acceso en red 11.4.1. Política de uso de los servicios de red	Se debería proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar.	Jefe de Sistemas
	11. Control de Accesos 11 4 Control de acceso en red 11.4.7. Control de encaminamiento en la red	Se deberían establecer controles de enrutamiento en las redes para asegurar que las conexiones de los ordenadores y flujos de información no incumplen la política de control de accesos a las aplicaciones de negocio.	Jefe de Sistemas
9	11. Control de Accesos 11 2 Gestión de acceso de usuario 11.2.4. Revisión de los derechos de acceso de los usuarios	El órgano de Dirección debería revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.	Jefe de Sistemas
	11. Control de Accesos 11 4 Control de acceso en red 11.4.4. Protección a puertos de diagnóstico remoto	Se debería controlar la configuración y el acceso físico y lógico a los puertos de diagnóstico.	Jefe de Sistemas
9	09. Seguridad Física y del Entorno 9 1 Áreas seguras 9.2.1. Instalación y protección de equipos	El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado.	Jefe de Sistemas

9	11. Control de acceso 11.6 Control de acceso a las aplicaciones y a la información. 11.6.1. Restricción de acceso a la información	Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.	Jefe de Sistemas
9	15.Cumplimiento 15.1 Conformidad con los requisitos legales 15.1.3. Salvaguarda de los registros de la Organización	Los registros importantes se deberían proteger de la pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios, regulaciones, contractuales y de negocio	Jefe de Sistemas
9	10. Gestión de Comunicaciones y Operaciones 10.5 Copias de seguridad. 10.5.1 Copias de seguridad de la	Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de	Jefe de Sistemas
9	15. Conformidad 15 1 Conformidad con los requisitos legales 15.1.3. Salvaguarda de los registros de la	Los registros importantes se deberían proteger de la pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios, regulaciones, contractuales	Jefe de Sistemas
9	09. Seguridad Física y del Entorno 9 1 Áreas seguras 9.2.1. Instalación y protección de equipos	El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no	Jefe de Sistemas
	9. Seguridad física y del entorno 9.2 Seguridad de los equipos 9.2.2. Suministro eléctrico	Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo.	Jefe de Sistemas
	9. Seguridad física y del entorno 9.2 Seguridad de los equipos 9.2.4. Mantenimiento de equipos	Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Jefe de Sistemas
9	08. Seguridad ligada a los Recursos Humanos 8 2 Seguridad en el desempeño de las funciones del empleo 8.2.3. Procedimiento disciplinario	Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad.	Jefe de Sistemas
9	11. Control de Accesos 11 5 Control de acceso al sistema operativo 11.5.2. Identificación y autenticación de usuario	Todos los usuarios deberían disponer de un único identificador propio para su uso personal y exclusivo. Se debería elegir una técnica de autenticación adecuada que verifique la identidad reclamada por un usuario.	Jefe de Sistemas
9	08. Seguridad ligada a los Recursos Humanos 8 2 Seguridad en el desempeño de las funciones del empleo 8.2.2. Formación y capacitación en seguridad de la información	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo	Jefe de Sistemas